UNIVERZITET SINGIDUNUM
BEOGRAD
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

DOKTORSKA DISERTACIJA

# SINTEZA JEDNE KLASE POUZDANIH KRIPTOGRAFSKIH ALGORITAMA ZA SISTEME SA OGRANIČENIM RESURSIMA

**Mentor**:

Prof. dr. Milan Milosavljević

**Student**:

Tomislav B. Unkašević

Broj indeksa:
460030/2018

Beograd, 2021.

SINGIDUNUM UNIVERSITY
BELGRADE
DEPARTMENT FOR POSTGRADUATE STUDIES

DOCTORAL DISSERTATION

# SYNTHESIS OF ONE CLASS OF RELIABLE CRYPTOGRAPHIC ALGORITHMS FOR SYSTEMS WITH LIMITED RESOURCES

**Mentor**:

Prof. dr. Milan Milosavljević

**Student**:

Tomislav B. Unkašević

Index number:
460030/2018

Belgrade, 2021.

**Mentor**:

Prof. dr. Milan Milosavljević, redovni profesor
Univerzitet Singidunum

**Članovi komisije**:

Prof. dr. Milan Milosavljević, redovni profesor
Univerzitet Singidunum

Prof. dr. Mladen Veinović, redovni profesor
Univerzitet Singidunum

Prof. dr. Branko Kovačević, profesor emeritus
Univerzitet u Beogradu, Elektro-tehnički fakultet

**Datum odbrane**: _____

*Prof. dr. Miloradu Obradoviću, generalu u penziji*

*i*

*Prof. dr. Milanu Milosavljeviću, redovnom profesoru*

# Zahvalnica

Izrada i završetak ovog rada rezultat je velike podrške koju sam u tom procesu imao.

Veliku i nesebičnu zahvalnost dugujem profesoru doktoru Miloradu Obradoviću koji me je svojim znanjem, iskustvom i veštinom podstakao da krenem u izradu ovoga rada i u tom procesu podržao na svaki način. Njegovo iskustvo i saveti pomogli su mi da se svaka dilema i situacija razreši na najefikasniji i najsvrsishodniji mogući način.

Doktor Vladimir Cizelj je ukazavši mi priliku da svoje profesionalno delovanje nastavim u izazovnom i stimulativnom istraživačkom okruženju Instituta VLATACOM suštinski podržao i inicirao izradu ovoga rada. Njegovo poverenje i podrška u toku doktorskih studija omogućili su miran i stabilan istraživački proces kojim je rezultirao ovaj rad. Stvaranjem uslova za izradu ovog rada i pruženom podrškom u toku njegove izrade esencijalno je uticao na realizaciju ovog rada na čemu mu se duboko zahvaljujem.

Svojim iskusnim i dragocenim vođenjem kroz doktorske studije kao mentor profesor doktor Milan Milosavljević je učinio da učenje i istraživanje poprimi formu radosti i zadovoljstva otkrivanja. Diskusije i rasprave u toku izbora teme i u toku njene obrade obojile su ovaj rad. Stimulativnost njegovog vođenja u ogromnoj meri je olakšala i obojila ovaj period. Veliko hvala na stečenom iskustvu i nadam se barem ponešto usvojenog metoda vođenja.

Članovima komisije za pregled i odbranu rada, profesorima doktorima Branku Kovačeviću i Mladenu Veinoviću zahvaljujem se na pažljivom pregledu rada i sadržajnim primedbama koje su učinile da rad bude vizuelno i sadržajno bolji.

Zahvaljujem se kolegi i komentoru u Institutu VLATACOM doktoru Zoranu Banjcu na sadržajnim diskusijama u pogledu izgleda i sadržaja rada, kao i na iskazanim primedbama na prvu verziju rada. Njegove primedbe su učinile ovaj rad sadržajnijim.

Zahvaljujem se kolegi doktoru Miroslavu Periću i pripadnicima kripto-grupe Instituta VLATACOM na iskazanoj podršci, pažnji i razumevanju tokom mojih doktorskih studija i izrade ovog rada.

Na kraju zahvaljujem se članovima moje porodice koji su u svakoj situaciji podržali moja profesionalna opredeljenja i sa razumevanjem pratili i podržali moje profesionalne potreba čak i kada to za njih nije bilo najbolje. Takvim svojim stavom omogućili su stabilno porodično i profesionalno okruženje na čemu im još jednom zahvaljujem.

**Naslov disertacije**: Sinteza jedne klase pouzdanih kriptografskih algoritama za sisteme sa ograničenim resursima

**Rezime**: Za realizaciju informacione bezbednosti u sajber prostoru potrebno je definisati kriptografske algoritme koji omogućavaju visok stepen zaštite podataka i komunikacija, podržavaju veoma velike komunikacione brzine, zahtevaju ekstremno male procesne resurse i imaju izuzetno kompaktnu implementaciju. Ove karakteristike upućuju na klasu sekvencijalnih kriptografskih algoritama odnosno sintezu pseudoslučajnih generatora sa prethodno navedenim karakteristikama. Imajući u vidu navedene zahteve cilj ovog rada je sinteza klase pouzdanih i efikasnih pseudoslučajnih generatora. Definisana je klasa slučajnih procesa baziranih na promenljivim permutacijama i analizirane su probabilističke i statističke osobine definisane klase slučajnih procesa. Definisana klasa slučajnih procesa poslužila je kao referentni model za definisanje klase pseudoslučajnih generatora parametrizovane sa dva pseudoslučajna niza. Koristeći teoriju verovatnoće, teoriju informacija i teoriju brojeva analizirane su osobine definisane klase pseudoslučajnih generatora. Izvedeni su dovoljni uslovi pod kojima izlazni niz definisane klase pseudoslučajnih generatora ima asimptotski uniformnu raspodelu ima izlaznih simbola. Korelaciona analiza je pokazala da su elementi parametrizujućih sekvenci i izlaznog niza asimptotski nezavisni i kao posledicu toga imamo da količina informacija koju element izlaznog niza nosi o tekućem unutrašnjem stanju generatora je asimptotski nula. Analiza perioda je pokazala da kada se parametrizujuće sekvence odaberu na odgovarajući način period generisanog izlaznog niza postaje značajno veći od perioda parametrizujućih sekvenci. Navedene osobine spadaju u neophodne osobine kriptografskih pseudoslučajnih generatora. Efikasnost predložene konstrukcije se postiže odabirom efikasnih pseudoslučajnih generatora, na primer sekvenci generisanih višestrukim linearnim pomeračkim registrima. U radu su navedene i moguće primene predložene klase pouzdanih pseudoslučajnih generatora.

**Ključne reči**: kriptografski algoritmi, sinteza kriptografskih algoritma, statistička analiza, korelacija, period, prelivanje informacija

**Dissertation title**: Synthesis of one class of reliable cryptographic algorithms for systems with limited resources

**Abstract**: For the information security in the cyber space it is necessary to define cryptographic algorithms that enable a high degree of data and communication protection, support very high communication speeds, require extremely small processing resources and have an extremely compact implementation. These characteristics point to a class of sequential cryptographic algorithms, i.e. the synthesis of pseudorandom generators with the aforementioned characteristics. Having in mind the stated requirements, the aim of this work is the synthesis of a class of reliable and efficient pseudorandom generators. A class of random processes based on variable permutations is defined and the probabilistic and statistical properties of the defined class of random processes are analysed. The defined class of random processes served as a reference model for defining the class of pseudorandom generators parameterized with two pseudorandom sequences. Using probability theory, information theory and number theory, the properties of a defined class of pseudorandom generators are analysed. Sufficient conditions under which the output sequence of the defined class of pseudorandom generators has an asymptotically uniform distribution of output symbols are derived. Correlation analysis showed that the elements of the parameterizing sequences and the output sequence are asymptotically independent and as a consequence we have that the amount of information that the element of the output sequence carries about the current internal state of the generator is asymptotically zero. Analysis of the output sequence period showed that when the parameterizing sequences are selected appropriately, the period of the generated output sequence becomes significantly larger than the period of the parameterizing sequences. These properties are the necessary features of cryptographic pseudorandom generators. The efficiency of the proposed construction is achieved by its compactness and selection of efficient pseudo randomly generated parametrizing sequences, for example sequences generated by multiple linear shift registers. The possible applications of the proposed class of reliable pseudorandom generators are listed.

**Keywords**: cryptographic algorithms, synthesis of cryptographic algorithms, statistical analysis, correlation, period, information leakage

# Sadržaj

# Glava 1

# Uvod

Pojava računara i njihov tehnološki razvoj značajno su izmenili način života ljudi i uticali na razvoj civilizacije. Prvobitno su računari imali pasivnu ulogu uređaja za skladištenje, obradu i čuvanje podataka. Tehnološki napredak u razvoju računarskih komponenti omogućio je ogromno poboljšanje računarskih performansi u smislu kapaciteta i brzine obrade podataka kao i enormno povećanje mogućnost za skladištenje podataka. Povećanje brzine i kapaciteta obrade podataka dovelo je do mogućnosti razvoja i implementacije složenijih algoritama mašinskog učenja i veštačke inteligencije. Na tim osnovama razvijeni su složeni informacioni sistemi čijom primenom se uticaj računarskih tehnologija na život ljudi postepeno povećavao i širio na različite oblasti društva. Novi tehnološki bum sredinom devedesetih godina prošlog veka demonstriran kroz razvoj mikroprocesorskih i komunikacionih tehnologija postepeno je učinio da mikroprocesorski uređaji, informacioni sistemi i njihove mreže aktivno utiču na naše životne aktivnosti. Danas je gotovo nezamisliva bilo koja ljudska aktivnost u kojoj mikroprocesorski uređaji ne doprinose pouzdanosti, kvalitetu i efikasnosti delovanja te i tako utiču na nivo kvaliteta života svakog pojedinca. U funkcionisanju društva to se ogleda u primeni složenih sistema upravljanja u elektroprivredi, saobraćaju, industriji i drugde a u ličnom životu kroz lakoću upotrebe i kontrole različitih uređaja, na primer u domaćinstvu kontrolom upotrebe kućnih aparata, zagrevanja, osvetljenja i mehanizama obezbeđenja neposredno ili na daljinu upotrebom mobilnih komunikacionih uređaja. Na taj način stvorena je jedna simbiotska zajednica ljudi i mašina čijim uzajamnim interakcijama se realizuju različiti procesi i aktivnosti, sajber prostor. Deo sajber prostora koji odgovara mašinama/stvarima koje čine pojedinačne i složene sisteme naziva se Internet stvari (Internet of Things - IoT) [1–4] Na apstraktnom nivou

on se sastoji od jednostavnih uređaja, senzora koji su povezani sa mikroprocesorskim uređajima a ovi su pak povezani između sebe i sa složenijim procesorskim sistemima u kompleksne informacione sisteme. Shodno tome arhitektura jednog složenog sistema na apstraktnom nivou sastoji se od:

1. Elemenata koji detektuju i prikupljaju signale iz okoline, senzori;
2. Komunikacionog dela čija je uloga da prenosi podatke unutar sistema između elemenata sistema;
3. Procesni deo sistema koji podrazumeva ekstrakciju informacija, njihovu obradu i definisanje akcije sistema na osnovu sprovedene obrade.

Ovako uopšteno određeni sistemi se primenjuju u gotovo svim oblastima života, navešćemo samo neke od njih:

- **Primena u zdravstvenom sistemu** - Korišćenje nosivih senzorskih uređaja povezanih sa pacijentima za registrovanje zdravstvenih parametara omogućava lekarima da kontrolišu stanje pacijenta van bolnice i u realnom vremenu. Kroz kontinuirano nadgledanje odabranih pokazatelja omogućava se bolja i preciznija dijagnostika, primerenija i efikasnija terapijsko zbrinjavanje a u krajnjem slučaju prevencija smrtonosnih događaja kod visoko rizičnih pacijenata.
  Integracijom IoT tehnologija u bolničku opremu, kreveti, uređaji ..., olakšava se praćenje stanja pacijenata na bolničkom lečenju kroz automatizovano i kontinuirano praćenje njihovog stanja i pravovremenu i efikasnu reakciju zdravstvenog osoblja kada je to potrebno.
- **Nadgledanje i upravljanje saobraćajem** - Internet stvari može biti veoma koristan u upravljanju automobilskim saobraćajem u velikim gradovima, koncept pametnih gradova. Tu se stvari mogu posmatrati na više načina.
  Na individualnom nivou koristeći različite načine prikupljanja informacija, tekuća lokacija vozila, informacije vezane za saobraćaj u određenom geografskom okruženju, odredišna lokacija, i uz pomoć prikupljenih informacija optimizuje se putna ruta po vremenu, rastojanju ili ceni, na primer Google maps.
  Na globalnom nivou upotreba IoT infrastrukture i odgovarajućeg softvera u zavisnosti od vremenskih prilika, doba dana i drugih parametara upravlja se

gradskom signalizacijom kako bi se optimizovala propusna moć saobraćajnica i tako ubrzao promet vozila u ciljanom okruženju.
Na logističkom nivou, instalaciojom IoT uređaja u vozila ostvaruje se efikasna međusobna povezanost između vozila, vozača i operatera odgovornog za organizaciju prevoznog sistema. Na taj način su u svakom trenutku dostupne informacije o stanju i statusu vozila, njegova geografska lokacija i servisni podaci. Upotreba ovih podataka može doprineti značajnim uštedama u eksploataciji voznog sistema.

- **Unapređenje poljoprivredne proizvodnje -** Raspoređivanjem senzora na obradivim površinama dobijaju se informacije o stanju zemljišta i vazduha na njima. Prikupljene informacije se koriste u procesu uzgajanja poljoprivrednih kultura tako što se zemljištu i atmosferi dodaju odgovarajući elementi primereni fazama razvoja uzgajanih kultura. Time se omogućava sprečavanje razvoja bolesti na kulturama tokom rasta i povećanje nivoa prinosa.

- **Upravljanje distribucijom i upotrebom energije -** Sa distributivne tačke gledišta razmeštanjem senzora na odgovarajućim strateškim tačkama distributivne mreže električne energije se može ostvariti kontrola proizvodnje neophodne količine električne energije i njeno usmeravanje tako da sistem funkcioniše na ekonomičan način.
  Sa potrošačkog stanovišta instalacijom senzorskih sistema za kontrolu potrošnje električne energije korisnici mogu ostvariti zanačajne materijalne uštede. Uspostavljanje dvosmernog sistema komunikacije između distributera i potrošača dobijaju se korisne informacije o gubicima tokom distribucije, postojećim kvarovima i njihovom otklanjanju.

Ovih nekoliko navedenih ilustrativnih primera pokazuju mogućnosti koje IoT pruža za poboljšanje društvenog standarda i kvaliteta života. Naravno, sve je to pod pretpostavkom da sistem funkcioniše na način koji je predviđen. Sa druge strane u sredinama baziranim na primenama ovih i sličnih tehnologija osim ličnih u pitanju su i širi društveni interesi, proizvodnja i distribucija energije u energetskim sistemima, prerada i distribucija vode, proizvodnja i distribucija hrane ,

upravljanje kopnenim, vazdušnim i vodenim saobraćajem, jednom rečju kritična infrastruktura za funkcionisanje društva. Za stabilnost funkcionisanja zajednice neophodno je obezbediti neprekidnost i ispravnost njenog funkcionisanja.

U tom kontekstu, upravljanje procesima i donošenje odluka, integritet i bezbednost podataka imaju veoma važnu ulogu iz prostog razloga što je akcija/odluka adekvatna situaciji u meri u kojoj su podaci na osnovu kojih se odluka donosi/sprovodi verodostojni. Pored verodostojnosti i tačnosti podataka bitno je u takvim sistemima obezbediti i privatnost podataka kako zbog autonomije i pouzdanosti rada tako i zbog očuvanja zakonskih prava vlasnika i korisnika takvih sistema. Prema tome problemi koji se u skladu sa prethodno opisanim potrebama rešavaju mogu se generalno grupisati u četiri segmenta

- Privatnost podataka u sistemu koja se odnosi na to da podaci koji se kreiraju u sistemu budu dostupni samo i jedino ovlašćenim osobama u sistemu. To znači da kreator podataka, uređaj, osoba ili proces, podatke prosleđuje definisanom entitetu na način koji garantuje da će prosleđeni sadržaj biti dostupan jedino onome kome je namenjen. Ovaj zahtev se obezbeđuje primenom različitih kriptografskih tehnika zaštite podataka. Ovde treba primetiti da kada jedan entitet u sistemu dođe u posed nekog skupa podataka on ih može učiniti dostupnim nekim drugim entitetima u skladu sa definisanim pravima, ulogom i sistemskim bezbednosnim politikama.

- Identifikacija, autentifikacija i autorizacija entiteta u sistemu sprovodi se tako što svaki entitet dobija jedinstveni identifikator. Metod dodele identifikatora entitetima mora da bude takav da omogućava jedinstvenost identifikacije i onemogućava lažno predstavljanje odnosno falsifikovanja identiteta. Svaki entitet, prepoznatljiv po svom identitetu, u sistemu ima definisana prava i dozvoljene aktivnosti. Na osnovu dodeljenih identiteta u sistemu se primenom modernih kriptoloških tehnika definišu protokoli za identifikaciju i autentifikaciju entiteta. Po uspešnom sprovođenju procedura identifikacije i autentifikacije entitetu se dodeljuju prava pristupa i dozvoljene operacije u skladu sa sistemskim operativnim i bezbednosnim politikama.

- Integritet sistema se takođe može definisati i kontrolisati primenom modernih kriptoloških metoda. Na taj način se obezbeđuje da sistem zajedno sa uređajima i programskim okruženjem bude očuvan u stanju u kojem je uspostavljen i da sve promene budu detektovane. Ovde se podrazumeva da

postoje procedure koje omogućavaju izmene sistema, u odnosu na uređaje, korisnike i programsko okruženje, na taj način da se može očuvati i proveravati integritet sistema uspostavljen od strane ovlašćenih autoriteta, kreatora sistema.

- Dostupnost podataka znači da su podaci dostupni ovlašćenim korisnicima u trenutku kada su im potrebne. Slično poverljivosti i integritetu, dostupnost je takođe važna karakteristika sistema. Dostupnost je obično povezana sa pouzdanošću i vremenom neprekidnog rada sistema. Kontinuiranost rada sistema se obezbeđuje analizom rizika od otkaza i prema njoj projektovanoj redundansi sistem. Neprekidnost i ispravnost rada sistema može biti narušena zlonamernim informaciono bezbednosnim napadima na sistem i stoga moraju biti preduzete bezbednosne mere koje mogućnost tog tipa napada smanjuju ili umanjuju njegove posledice.

Moderna tehnologija zaštite informacionih sistema bazirana na kriptološkim metodama u stanju je da definiše i realizuje rešenja koja uspešno ispunjavaju prethodno navedene potrebe/zahteve ali same potrebe/zahtevi indukuju složenost rešenja koje se kreira. Drugim rečima složenost problema koji se rešava utiče na složenost kreiranog rešenja. Očekivano je da se složeni informacioni sistemi sastoje od elemenata različite procesne moći u smislu dostupnosti električne energije, procesorske snage i količine raspoložive memorije. Shodno tome i projektovana rešenja moraju uvažavati ograničenja koja implementaciono okruženje nameće [5–10]. U gotovo svakom bezbednosnom rešenju neku ulogu imaju pseudoslučajni generatori. Pseudoslučajni generatori se široko primenjuju u oblasti šifrovanja podataka sekvencijalnim kriptografskim algoritmima, "challenge response" protokolima, protokolima za generisanje kriptografskih ključeva i drugo. No, kao što praksa pokazuje nije lako dizajnirati kvalitetan pseudoslučajni generator. U slučaju kada je okruženje takvo da su dizajneru na raspolaganju ograničeni resursi izazov postaje još veći. U suštini, osnovni zahtev koji se nameće je da nije moguće prediktovati izlazni niz pseudoslučajnog generatora na osnovu nekog njegovog početnog odsečka. Metode koje se u toj analizi primenjuju uglavnom se odnose na statističke i algebarske tehnike. Shodno tome kvalitet samog generatora se procenjuje u odnosu na njegovu otpornost na pokušaje predikcije vrednosti izlaznoga niza u odnosu na kriptografske kriterijume kvaliteta pseudoslučajnih generatora.

Cilj ovog rada je dizajniranje klase pseudoslučajnih generatora sa dobrim kriptografskim osobinama. Sam rad se sastoji od pet poglavlja i spiska korišćene literature:

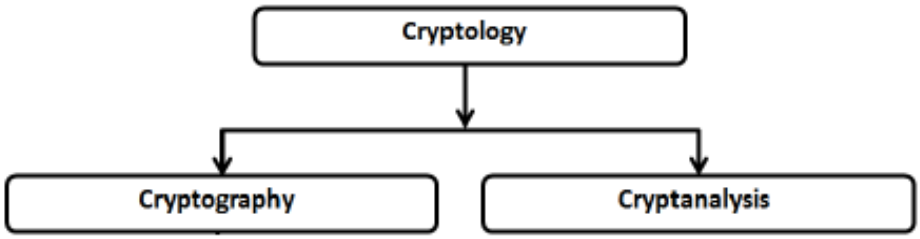
- U prvom delu rada, uvodnom razmatranju, ukratko je izložena motivacija za ovo istraživanje, problem koji se razmatra i njegov značaj, pristup njegovom rešavanju i struktura rada.
- U drugom delu daje se taksonomija i osnovne karakteristike kriptografskih algoritama, klasifikacija stepena bezbednosti, modeli za procenu bezbednosti kriptografskih algoritama i komparativna analiza opisanih modela za procenu bezbednosti kriptografskih algoritama.
- Treći deo se bavi analizom do sada poznatih konstrukcija baziranih na promenljivim permutacijama i njihovim bezbednosnim karakteristikama.
- Četvrti deo je centralni deo rada i sadrži opis klase pouzdanih sekvencijalnih kriptografskih algoritama za primenu u uređajima sa ograničenim resursima i njemu pridruženi matematički model. Takođe u ovom delu je sprovedena analiza bezbednosnih karakteristika predložene konstrukcije i komparativna analiza dobijenih rezultata sa algoritmima i slabostima opisanim u trećem delu. Dodatno, analizirane su i navedene mogućnosti primene definisane klase algoritama.
- Peti deo sadrži rezime rada, pregled glavnih doprinosa kao i pravce daljeg istraživanja u ovoj oblasti indukovanih otvorenim pitanjima u ovom istraživanju.

# Glava 2

# Kriptologija

## 2.1 Kriptologija, pojam i taksonomija

Od pojave pismenosti i prenosa poruka napisanih na različitim medijima javila se i potreba za prikrivanjem informacija koje poruke sadrže. Način transformacije poruke je takav da su informacije koje poruka sadrži dostupne samo onome kome je poruka namenjena. U tu svrhu primenjivale su se različite tehnike počev od transformacije grafičke reprezentacije poruke, zamena slova, do utiskivanja poruke u nosač poruke tako da je poruka neprimetna neupućenim osobama, nevidljivo mastilo. Proučavanje i razvoj metoda za prikriveno komuniciranje nazvano je kriptografija sa značenjem „tajno pisanje " od Grčkih reči $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma-$ što znači tajni, prikriveni i $\gamma\rho\acute{\alpha}\varphi\varepsilon\iota\upsilon-$ što znači pisanje. U slobodnom prevodu označava veštinu tajnog pisanja. Kriptografija kao ljudska aktivnost je vrlo stara i arheološki dokazi transformacije pisanih i slikovnih poruka datiraju se u period od 2000 godina pre nove ere, u doba stare Egipatske civilizacije, [16]. Vremenom, kako su se razvijali vidovi, sredstva i obim komunikacije raslo je i interesovanje za poznavanjem zaštićenog sadržaja onih kojima zaštićene informacije nisu bile namenjene. Ta potreba je potakla razvoj novih znanja i veština u oblasti tajnog komuniciranja a to je analiza zaštićenih poruka i razvoj metoda za rekonstrukciju zaštićenih informacija. Tako je u oblasti tajnog komuniciranja nastala kriptoanaliza, sestra bliznakinja kriptografije. Njihova veza je jedinstvena i neraskidivi jer je svaki napredak u bilo kojoj od te dve oblasti nužno indukovao napredak u onoj drugoj. Uzajamna povezanost kriptografije i kriptoanalize dovela je do formiranja jedinstvene oblasti, kriptologija, koja se bavi proučavanjem i razvojem tajnog komuniciranja na naučnim principima. Reč kriptologija je složenica nastala od grčke




Slika 2.1: Taksonomija kriptologije

reči $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma-$ što znači tajni, prikriveni i reči $\lambda\acute{o}\gamma o\varsigma-$ koja ima značenje nauka, znanje što u slobodnom prevodu označava nauku o tajnom komuniciranju, slika 2.1.

Kriptografija je započela svoj put sa ciljem zaštite informacija sadržanih u komunikacionim porukama ali je razvoj komunikacionih tehnologija učinio da se ciljevi prošire a mogućnosti obogate. Moderna kriptografija u današnjem komunikaciono umreženom svetu realizuje sledeće ciljeve:

- Poverljivost je funkcionalnost onemogućavanja pristupa informacionom sadržaju poruke svima osim ovlašćenih primalaca. Tajnost je pojam koji je sinonim za poverljivost i privatnost.

- Integritet podataka je funkcionalnost koja omogućava detekciju izmene podataka. Pod neovlašćenom manipulacijom podacima podrazumeva se umetanje, brisanje i zamena sadržaja podataka koju vrše lica bez ovlašćenja za takav vid operacija nad podacima. Takođe, moguća je i nenamerna izmena podataka usled grešaka na prenosnom putu.

- Autentifikacija je funkcionalnost koja se odnosi na identifikaciju i potvrdu identiteta entiteta koji učestvuju u komunikaciji. Ova funkcionalnost omogućava stranama koje stupaju u komunikaciju da se uvere u identitet suprotne strane, poreklo i vreme nastanka poruka.

- Neporecivost aktivnosti je funkcionalnost koja sprečava entitet da negira prethodne radnje u komunikaciji. Ova funkcionalnost omogućava pouzdano utvrđivanje iniciranih radnji i transakcija tako da u slučaju da neka od strana u komunikacija pokuša da porekne svoje aktivnosti analizom poruka se nedvosmisleno utvrđuje tačnost poricanja.

Kriptologija proučava i konstruiše transformacije poruka čija primena omogućava navedene ciljeve.

Transformacije poruka definišemo na sledeći način.

Označimo sa $A = \{a_1, a_2, ..., a_l\}$ proizvoljnu azbuku čiji su simboli $a_1, a_2, ..., a_l$. Tada sa $A^i = \{x_1x_2...x_i \mid x_j \in A,\ j = 1, 2, ..., i\}$ označavamo skup svih reči dužine $i$ nad azbukom $A$ a sa $A^* = \bigcup_{i=0}^{\infty} A^i$ skup svih reči nad azbukom $A$.

Neka su sada date tri azbuke $M-$ azbuka poruka, $K-$ azbuka ključeva i $C-$ azbuka šifrata. Tada svako preslikavanje $F : K^* \times M^* \longrightarrow K^* \times C^*$ za koje važi $F(k, m) = (k, c)$ nazivamo transformacijom poruke $m$ primenom funkcije $F$ i ključa $k$. U literaturi je uobičajeno da se ključ $k$ smatra parametrom i to se naznačava sa $F_k(m) = c$.

Da bi se realizovale funkcionalnosti poverljivosti, integriteta, autentičnosti i neporecivosti transformacije moraju posedovati određena svojstva. Tako na primer da bi se realizovala privatnost za datu funkciju $F$ koju zovemo funkcija šifrovanja mora da postoji funkcija $F^{-1}$ koju zovemo funkcija dešifrovanja i važi

$$F^{-1}(k_2,\ F(k_1, m)) = (k_1, m). \tag{2.1}$$

Funkcija šifrovanja se obično označava sa $E$ a funkcija dešifrovanja sa $D$ pa prethodna jednakost može da se piše i na sledeći način

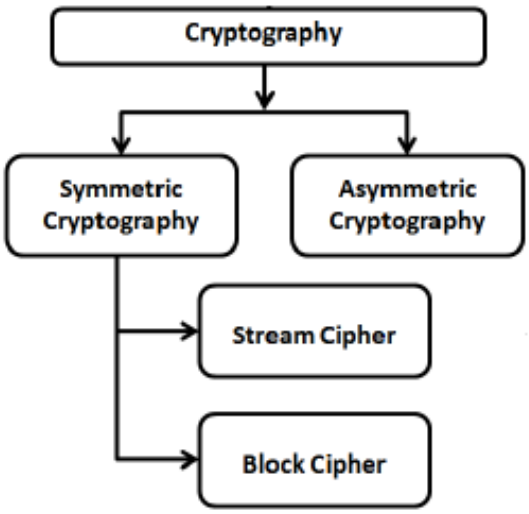
$$D_{k_2}(E_{k_1}(m)) = m \tag{2.2}$$

Transformacije šifrovanja i dešifrovanja se uobičajeno nazivaju kriptografski algoritmi.

## 2.2 Klasifikacija kriptografskih algoritama

Klasifikacija kriptografskih algoritma se vrši u odnosu na vrednosti kriptografskih ključeva $k_1$, $k_2$ koji se koriste za šifrovanje i dešifrovanje, jednakost (2.1). Klasa kriptografskih algoritama kod kojih su ključevi $k_1$ i $k_2$ jednaki naziva se klasom simetričnih kriptografskih algoritama. Klasa kriptografskih algoritama kod kojih su ključevi $k_1$ i $k_2$ različiti naziva se klasom asimetričnih kriptografskih algoritama. Klasifikacija kriptografskih algoritama je prikazana na slici 2.2.

Kako je tema ovoga rada sinteza simetričnih sekvencijalnih kriptografskih algoritama nećemo se upuštati u karakterizaciju i osobine asimetričnih kriptografskih algoritama.




Slika 2.2: Grafički prikaz taksonomije kriptografije

### 2.2.1 Simetrični kriptografski algoritmi

Simetrični kriptografski algoritmi za šifrovanje i dešifrovanje koriste isti kriptografski ključ što za posledicu ima da vrednost upotrebljenog ključa može biti poznata samo stranama koje žele direktnu komunikaciju. U suprotnom, svako ko zna vrednost upotrebljenog kriptografskog ključa i primenjeni kriptografski algoritam može doći do zaštićenih podataka. Zbog toga se ova klasa kriptografskih algoritama naziva još i kriptografski algoritmi sa tajnim ključem. Uobičajeno je da se proces računanja jednog elementa šifrata naziva taktom, ovo ne treba pojmovno povezivati sa procesorskim taktom u računarskim uređajima.

Prema broju simbola poruke koji se šifruju u jednom taktu simetrični kriptografski algoritmi se dele na:

- Sekvencijalne kriptografske algoritme
- Blokovske kriptografske algoritme.

Kako je tema ovoga rada sinteza simetričnih sekvencijalnih kriptografskih algoritama nećemo se upuštati u karakterizaciju i osobine blokovskih kriptografskih algoritama.

### 2.2.2 Sekvencijalni kriptografski algoritmi

Konstrukcije koje po nekim karakteristikama podsećaju na moderne sekvencijalne kriptografske algoritma su se pojavile krajem devetnaestog i početka dvadese-

tog veka. Konačno uobličavanje modela sekvencijalnih kriptografskih algoritama odigralo se pod uticajem Šenonovog rada u oblasti teorije informacija i zaštite podataka [11]. Šenonov rad na matematičkom opisu elektronskih komunikacija i metoda njihove zaštite datira od druge decenije dvadesetog veka ali su rezultati tog rada bili klasifikovani kao značajni za odbranu i javno publikovani tek u [11]. 1948. godine.

U [11] Šenon je formulisao dva osnovna principa sinteze kriptografskih algoritama:

1. **Princip konfuzije** koji kaže da svaki simbol šifrata mora da zavisi na složen način od simbola kriptografskog ključa i simbola poruke koja se šifruje. Teorijski i praktično govoreći smisao ove zavisnosti leži u otežavanju rekonstrukcije primenjenog kriptografskog ključa čak i uz poznatu primenjenu transformaciju. Na taj način posedovanje šifrata protivniku ne omogućava otkrivanje primenjenog kriptografskog ključa niti poruke koja se šifruje jer se informacije o primenjenom ključu i poruci prekrivaju uzajamnom interakcijom simbola ključa i poruke.

2. **Princip difuzije** koji kaže da simboli šifrata treba da zavise na takav način od kriptografskog ključa i simbola poruke da ako se izmeni jedan simbol poruke koja se šifruje tada se u šifratu izmenjene poruke menja polovina simbola šifrata. Smisao principa difuzije je da onemogući prelivanje statističkih osobina jezika kojem poruka koja se šifruje pripada u statističke osobine šifrata.

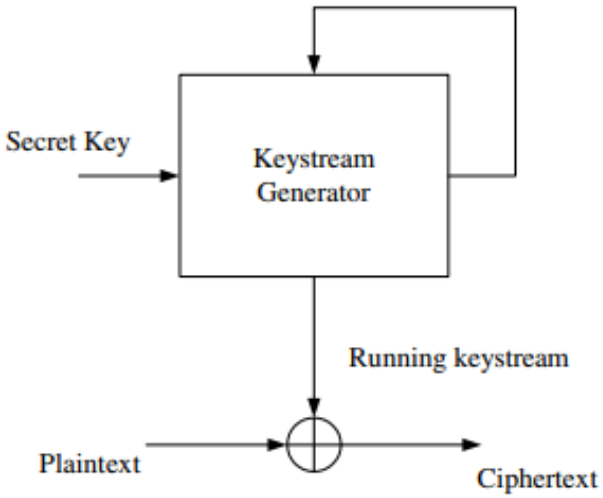
Primenjujući ova dva principa Šenon je definisao sistem „One time pad" (OTP) koji se primenjuje pod sledećim uslovima:

1. Simboli ključa se generišu na slučajan način,

2. Dužina primenjenog ključa jednaka je dužini poruke koja se šifruje,

3. Za svako poruku koristi se novi ključ, različit od svih prethodno primenjenih.

Ukoliko su prethodno navedeni uslovi ispunjeni pri šifrovanju OTP sistemom može se pokazati da ne postoji način za otkrivanje sadržaja poruke bez poznavanja primenjenog ključa, sistem je apsolutno bezbedan.




Slika 2.3: Grafički prikaz aditivnog sekvencijalnog kriptografskog algoritma

Šenonov sistem je nepraktičan za primenu u komunikacionim mrežama sa velikim brojem učesnika jer se pojavljuje problem sa distribucijom ključeva pouzdanim kanalima. Za sistem sa $n$ učesnika neophodno je generisati i distribuirati na pouzdan način $O(n^2)$ kriptografskih ključeva. Ideja koja je omogućila da se delimično prevaziđu ove teškoće je relaksacija zahteva da elementi ključa budu generisani slučajno i da se umesto toga simboli ključa generišu upotrebom pseudoslučajnih generatora a da se šifrovanje nadalje obavlja po Šenonovom modelu,

Teorija pseudoslučajnih generatora je u potpunosti formalno razvijena i definicije, osnovne karakteristike i reference na detaljniju literaturu se mogu naći u [12]. Neformalno govoreći generatori pseudoslučajnih nizova su deterministički algoritmi koji na osnovu relativno kratkih inicijalnih podataka, u slučaju šifrovanja i dešifrovanja-kriptografskog ključa, produkuju niz simbola proizvoljne dužine čiji elementi "izgledaju" kao da su odabrani na slučajan način, slika 2.3. Ova relaksacija sa sobom nosi i odgovarajuće posledice. Sekvencijalni kriptografski algoritmi ne mogu dostići nivo Šenonovog OTP sistema odnosno apsolutnu bezbednost, već spadaju u klasu praktično sigurnih kriptografskih algoritama. Detaljnije o modelima kriptografske bezbednosti i njihovoj klasifikaciji će biti reči u delu 2.4.

Koristeći Šenonove ideje razvijen je model sekvencijalnih kriptografskih algoritama koji po svojoj strukturi mogu biti, i najčešće jesu, složenije transformacije od onih viđenih u Šenonovim radovima.

Uopšteno govoreći sekvencijalni kriptografski algoritmi funkcionišu tako što se

nezavisno od elemenata poruke generiše pseudoslučajni niz koji se potom koristi za transformaciju poruke u šifrat. Da bi se poruka zaštićena sekvencijalnim kriptografskim algoritmom uspešno dešifrovala mora se nad šifratom uz korišćenje elemenata izlaznog niza pseudoslučajnog generatora sprovesti operacija inverzna transformaciji šifrovanja.

Pri tome redosled simbola šifrata i elemenata izlaznog niza pseudoslučajnog generatora mora biti istovetan kao pri šifrovanju. Otuda sledi da ti elementi moraju biti usklađeni po redosledu, sinhronizovani. U odnosu na to svojstvo sekvencijalni kriptografski algoritmi se dele na eksterno sinhronizovane sekvencijalne kriptografske algoritme i samosinhronizujuće sekvencijalne kriptografske algoritme

U opisu i izvođenju njihovih osobina obično se primenjuje algebra i teorija konačnih automata, [13], [14].

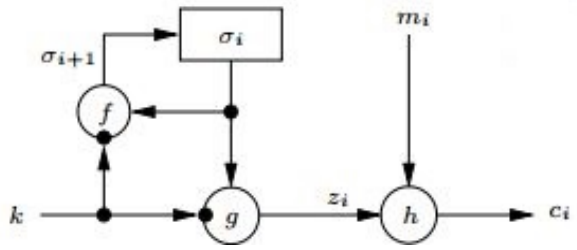
#### 2.2.2.1 Eksterno sinhronizovani sekvencijalni kriptografski algoritmi

U slučaju eksterno sinhronizovanih sekvencijalnih kriptografskih algoritama sinhronizacija redosleda elemenata izlaznog niza i elemenata šifrata održava se nekim eksternim mehanizmom. Mogu se, na primer, umetati brojači kao markeri blokova, formatiranje poruka i raspoznavanje formata ili neki drugi mehanizmi. Šifrovanje primenom eksterno sinhronizovanih sekvencijalnih kriptografskih algoritama se u opštem slučaju opisuje sledećim sistemom jednačina

$$\begin{aligned} \sigma_{i+1} &= f(\sigma_i, k) \\ z_i &= g(\sigma_i, k) \\ c_i &= h(z_i, m_i) \end{aligned} \tag{2.3}$$

gde funkcija $f$ predstavlja funkciju promene stanja, $g$ je funkcija koja generiše izlazni niz generatora a funkcija $h$ je funkcija šifrovanja. Nizovi $\sigma_i$, $z_i$, $c_i$ $i = 1, 2, 3, ....$ predstavljaju nizove unutrašnjih stanja generatora, izlazni niz generatora i elemente šifrata redom. Na slici 2.4 je prikazano šifrovanje ovim tipom kriptografskih algoritama.

$$\begin{aligned} \sigma_{i+1} &= f(\sigma_i, k) \\ z_i &= g(\sigma_i, k) \\ m_i &= h^{-1}(z_i, c_i) \end{aligned} \tag{2.4}$$




Slika 2.4: Proces šifrovanja eksterno sinhronizovanim sekvencijalnim kriptografskim algoritmom, [15]

a grafički prikaz procesa dešifrovanja je dat na slici 2.5.

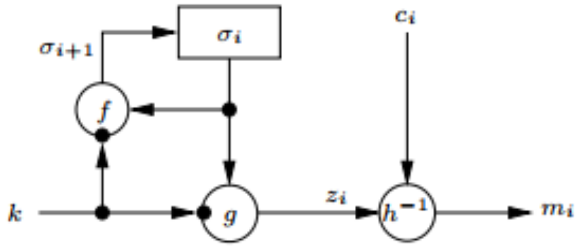
Osnovne karakteristike eksterno sinhronizovanih sekvencijalnih kriptografskih algoritama su:

1. Da bi pošiljalac i primalac mogli da komuniciraju, primalac mora biti u stanju da dešifruje primljenu poruku. Za to moraju biti ispunjeni sledeći uslovi:

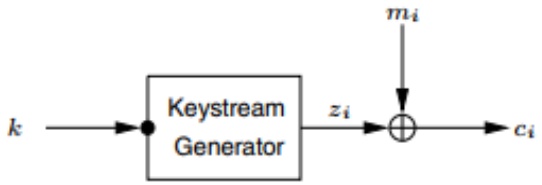
   - Pošiljalac i primalac moraju koristiti isti kriptografski ključ
   - Pošiljalac i primalac moraju biti sinhronizovani u radu to jest u svakom taktu moraju koristiti jednaka unutrašnja stanja.

2. Ovaj tip kriptografskih transformacija je otporan na greške u prenosu koje su različite od brisanja ili umetanja simbola. Greška na jednom primljenom simbolu izaziva grešku dekriptovanja samo na poziciji pogrešno primljenog simbola i ne prenosi se na ostatak poruke.

3. Napadi na sistem ovog tipa koji se manifestuju umetanjem ili brisanjem simbola šifrata lako se detektuju na prijemnoj strani kao gubitak sinhronizacije i nemogućnost dešifrovanja primljene poruke.




Slika 2.5: Proces dešifrovanja eksterno sinhronizovanim sekvencijalnim kriptografskim algoritmom, [15]




Slika 2.6: Proces šifrovanje u aditivnim sekvencijalnim kriptografskim algoritmima, [15]

U praksi se poruke najčešće predstavljaju u binarnom obliku a kao funkcija transformacije $h$ na slici 2.4 se koristi operacija ekskluzivne disjunkcije $\oplus$. Takvi sistemi se nazivaju aditivni sekvencijalni kriptografski sistemi i njihov rad je grafički prikazan na slikama 2.6 i 2.7

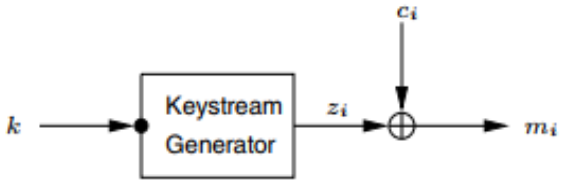
#### 2.2.2.2 Samosinhronizujući sekvencijalni kriptografski algoritmi

Samosinhronizujući sekvencijalni kriptografski algoritmi, koristi se i naziv asinhroni sekvencijalni kriptografski algoritmi, su kriptografski algoritmi kod kojih se šifrat generiše kao funkcija ključa i nekog broja prethodnih simbola šifrata. Operacija šifrovanja se u ovom tipu kriptografskih algoritama opisuje sledećim sistemom jednačina:

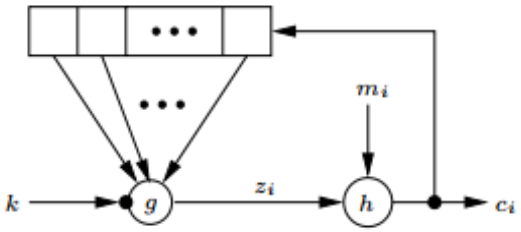
$$\begin{aligned} \sigma_{i+1} &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}) \\ z_i &= g(\sigma_i, k) \\ c_i &= h(z_i, m_i) \end{aligned} \tag{2.5}$$

Proces šifrovanja samosinhronizujućih sekvencijalnih kriptografskih algoritama je grafički prikazan na slici 2.8

Proces dešifrovanja šifrovanja samosinhronizujućih sekvencijalnih kriptografskih algoritama se opisuje sledećim sistemom jednačina:




Slika 2.7: Proces dešifrovanje u aditivnim sekvencijalnim kriptografskim algoritmima, [15]



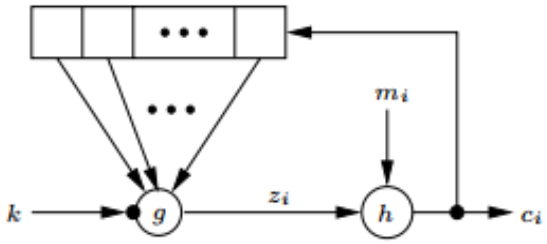

Slika 2.8: Proces šifrovanja samosinhronišućih kriptografskih algoritama, [15]

$$\begin{aligned} \sigma_{i+1} &= (c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}) \\ z_i &= g(\sigma_i, k) \\ m_i &= h^{-1}(c_i, m_i) \end{aligned} \tag{2.6}$$

a grafički prikaz je dat na slici 2.9

Osnovna i najvažnija karakteristika samosinhronizujućih sekvencijalnih kriptografskih algoritama je njihova sposobnost samosinhronizacije. To svojstvo se postiže načinom konstrukcije kriptografskih algoritama ovog tipa. Suština konstrukcije je u tome da se svako sledeće stanje konačnog automata kojim se opisuje ovaj tip kriptografskih algoritama sastoji od nekoliko poslednjih simbola šifrata, u sistemima jednačina (2.5) i (2.6) taj broj elemenata je $t$ a elementi su $c_{i-t}, c_{i-t+1}, \ldots, c_{i-1}$. Ova konstrukcija donosi nekoliko prednosti:

- Zahvaljujući ovakvom konstrukcionom pristupu prilikom dešifrovanja proces se samosinhronizuje po ispravnom prijemu $t$ simbola šifrata, tada konačni automat koji odgovara kriptografskom algoritmu dospeva u ispravno unu-




Slika 2.9: Proces dešifrovanja u samosinhronizujućim sekvenicjalnim kriptografskim algoritmima, [15]

trašnje stanje i proces ispravnog dešifrovanja se dalje nastavlja na regularan način.

- Ovaj tip šifrovanja je, iz istih razloga, otporan na greške u prenosu šifrata koje obuhvataju izmenu brisanje ili umetanje simbola šifrata. Prilikom dešifrovanja greška se prostire najdalje $t$ simbola od poslednjeg primljenog pogrešnog simbola šifrata.

- U ovakvim konstrukcijama u transformaciji simbola poruke učestvuju i simboli šifrata. Sprezanjem simbola šifrata sa simbolima poruke koja se transformiše onemogućava se prenos statističkih osobina jezika kojem poruka pripada na elemente šifrata. Ako je kriptografski algoritam dobro konstruisan na ovaj način se sprečavaju kriptografski napadi zasnovani na redundansi jezika kojem pripada skup poruka koje se transformišu.

Greške u procesu dešifrovanja, kao i u prethodnom slučaju, pored gubitka sinhronizacije mogu biti i indikator aktivnih napada na prenosni sistem.

## 2.3 Sinteza sekvencijalnih kriptografskih algoritama

U ovom delu su predstavljeni osnovni principi sinteze sekvencijalnih kriptografskih algoritma i osnovne komponente koje omogućavaju postizanje ciljeva apostrofiranih tim principima. Ostvarivanje ciljeva koje osnovni principi sinteze kriptografskih algoritama proklamuju nije samo po sebi garancija postizanja dobrih bezbednosnih karakteristika i o proceni bezbednosnihi kvaliteta kriptografskih algoritma biće više reči kasnije.

Dostignute brzine u prenosu podataka i intenzivan razvoj informatičkih i mrežnih tehnologija podstakle su procese digitalizacije društva. Za uspešnu i efikasnu digitalizaciju poslova, društvenih i ekonomskih procesa neophodno je realizovati bezbednosne mehanizme koji će te procese načiniti realno primenljivim. U mrežnom svetu pred kriptologiju, koja je kamen temeljac informacione bezbednosti, postavljaju se novi izazovi. Povećani bezbednosni zahtevi i održavanje visokih komunikacionih brzina uz redukciju cene primene adekvatnih rešenja samo su deo od njih. Sekvencijalni kriptografski algoritmi u tom pogledeu predstavljaju značajnu

gradivnu komponentu svake informaciono-bezbednosne arhitekture. U cilju uspostavljanja interoperabilnosti neki sekvencijalni kriptografski algoritmi sa dobrom reputacijom su bili uključeni u međunarodne telekomunikacione standarde, kao što su RC4 sekvencijalni kriptografski algoritam u IEEE 802.11 standardu za bežične mrežne komunikacije [17], A5/1 sekvencijalni kriptografski algoritam za Evropske GSM sisteme [18], SNOW 3G [19] i ZUC [20] sekvencijalni kriptografski algoritmi u 3GPP standardu, E0 sekvencijalni kriptografski algoritam za Bluetooth sisteme [21]. U cilju daljeg poboljšanja interoperabilnosti i unifikacije primenljivih kriptografskih rešenja pokrenuto je i realizovano nekoliko međunarodnih konkursa za sintezu pouzdanih kriptografskih algoritama za različite namene:

- NESSIE (New European Schemes for Signature, Integrity and Encryption) [22] je bio istraživački projekat u okviru Information Societies Technology (IST) Programme Evropske unije. Projekat je započet u januaru 2000 godine i trajao je do februara 2003 godine. Cilj projekta NESSIE bio je definisanje skupa pouzdanih kriptografskih algoritama koji bi bio formiran nakon javnog i transparentnog proces bezbednosne evaluacije predloga pristiglih na objavljeni javni konkurs. Predloge podnete za simetrične sekvencijalne kriptografske algoritme kreirali su poznati kriptolozi sa značajnom reputacijom u sintezi i analizi kriptografskih algoritama. Njihova rešenja su pokazala zavidne performanse i efikasnost ali ni jedno nije uspelo da zadovolji bezbednosne kriterijume zahtevane konkursnom dokumentacijom uključujući relativno poznate SNOW 1.0 [23], [24], LILI-128 [25]. Ni jedno od predloženih rešenja nije se kvalifikovalo kao preporučeno rešenje zbog slabosti detektovanih u procesu evaluacije [26–28]. I pored toga treba istaći da je NESSIE projekat imao veliki značaj jer je pomogao da se smanji uvek postojeći jaz između teorije i prakse. Dodatni značaj ovog projekta leži u pokretanju procesa unifikacije bezbednosnih zahteva i njihovog uticaja na procedure standardizacije bezbednosnih rešenja.

- Japanska vlada je 1999 obznanila da planira da državna administracija pređe na funkcionisanje po modelu elektronske državne uprave (eGovernment) zaključno sa 2003. godinom. U cilju realizacije tog plana i primeni adekvatnih bezbednosnih mehanizama 2000. godine je osnovano telo CRYPTREC (Cryptography Research and Evaluation Committee) za evaluaciju kriptografskih algoritama kako bi se dobila adekvatna rešenja za realizaciju

e-Government sistema [29]. Ovo organizaciono telo je pokrenulo projekat pod istim imenom i spisak prihvaćenih rešenja je objavljen u [30]. Kako napredak nauke i tehnologije nosi potrebu za praćenjem i usavršavanjem postojećih rešenja ovaj projekat se odvija kontinuirano. Pravci i ciljevi daljeg rada CRYPTREC projekta dati su u [31].

- Iskustva stečena na projektu NESSIE [22] u sintezi simetričnih sekvencijalnih kriptografskih algoritama kao i rastuća potreba za mehanizmima zaštite u sajberprostoru podstakli su Evropsku mrežu za napredak u kriptologiji ( European Network of Excellence for Cryptology-ECRYPT) da pokrene projekat eSTREAM [32] sa ciljem definisanja novih pouzdanih sekvencijalnih kriptografskih algoritama. Finalni izveštaj eSTREAM [34] projekta sadrži sedam preporučenih rešenja, tri hardverska Grain-v1 [35], Trivium [36], Mickei-v2 [37], kao i četiri definisana kao softverska Salsa 20/12 [34], Sosemanuk [38], Rabbit [39], HC-128 [40]. eSTREAM projekat izvršio je značajan uticaj u oblasti sinteze sekvencijalnih simetričnih kriptografskih algoritama svojim metodičnim pristupom i formalnom specifikacijom zahteva.

Prethodno pomenuti projekti ilustruju nekoliko stvari.

U prvom redu ukazuju na složenost problematike sinteze kvalitetnih sekvencijalnih kriptografskih algoritama. Koliko je problem složen i osetljiv vidi se iz izveštaja za sekvencijalne kriptografske algoritme projekta NESSIE gde nije odabrano ni jedno rešenje od predloženih iako su ih kreirali vrhunski kriptolozi sa respektabilnom reputacijom i rezultatima u kriptosintezi i kriptoanalizi. Značaj postojanja sigurnih simetričnih sekvencijalnih kriptografskih algoritama prepoznaje se u broju ovakvih projekata, dužini njihovog trajanja, sistematičnosti i angažovanim sredstvima. Po svemu izloženom može se slobodno zaključiti da oblast sinteze sekvencijalnih kriptografskih algoritma postaje jedno od centralnih pitanja moderne kriptologije.

### 2.3.1 Osnovne gradivne komponente sekvencijalnih kriptografskih algoritama

Veliki vremenski period je protekao od formiranja modela sekvencijalnih kriptografskih algoritama do danas. Uvažavajući Šenonove principe konfuzije i difuzije autori predloga i rešenja su ih realizovali na različite načine. Različiti načini de-

finisanja funkcija incijalizacije, promene stanja i elemenata izlaznog niza sekvencijalnih kriptografskih algoritama stvaraju utisak gotovo bezgranične šarolikosti u tom svetu. Međutim pažljiva analiza u pogledu njihove strukture i funkcionalnih celina pokazuje da se može izdvojiti skup transformacija čijim funkcionalnim povezivanjem se može opisati struktura i funkcionisanje gotovo svakog sekvencijalnog kriptografskog algoritma koji se pojavio u javnosti. Te strukture nazivamo osnovnim gradivnim komponentama sekvencijalnih kriptografskih algoritama i to su:

- Bulove funkcije
- Pomerački registri sa povratnom spregom
- ARX konstrukcije
- Promenljive permutacije.

Ova strukturna podela je zasnovana na apstraktnim svojstvima funkcionalnih celina a može imati različite implementacione oblike. Tako na primer promenljive permutacije mogu biti predstavljene kao obostrano jednoznačne vektorske Bulove funkcije i kao tablice permutacija ali zbog funkcionalnih osobina izdvojili smo ih kao karakterističnu gradivnu jedinicu. U ovom delu ćemo prikazati Bulove funkcije, pomeračke registre sa povratnom spregom i ARX konstrukcije. Promenljive permutacije i sa njima povezane konstrukcije biće prikazane u delu 3.

#### 2.3.1.1 Bulove funkcije

Bulove funkcije predstavljaju vrlo moćan alat u mnogim matematičkim disciplinama. Snaga tog alata leži u činjenicama da se svaki podatak može izraziti u binarnoj formi i da svaka numerička funkcija može da se predstavi kao vektorska Bulova funkcija. U kriptologiji Bulove funkcije se koriste kao funkcionalni elementi u algoritmima šifrovanja i dešifrovanja. Formalno Bulova funkcija od $n$ promenljivih se definiše kao preslikavanje $f : \{0,1\}^n \longrightarrow \{0,1\}$, $f(x_1, x_2, \ldots, x_n) = y$ gde $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ a $y \in \{0,1\}$. Bulove funkcije su proučavane sa različitih aspekata, u skladu sa potrebama oblasti u kojima se primenjuju tako da u vezi sa njima postoji obilje rezultata. Sa stanovišta kriptografije, proučavane su one osobine koje pomažu sintezu bezbednih kriptografskih algoritama i direktno utiču na bezbednost rešenja u kojima se primenjuju. Za kriptografske primene važne su sledeće osobine Bulovih funkcija:

- Svaka Bulova funkcija od $n$ promenljivih $f(x_1, x_2, \ldots, x_n)$ može se predstaviti kao polinom od $n$ promenljivih u skupu $\mathbb{F}_2[x_1, x_2, \ldots, x_n]$

$$f(x_1, x_2, \ldots, x_n) = \sum_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} a_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} \, x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n} \tag{2.7}$$

gde su $a_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} \in \{0, 1\}$ konstante a $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \{0, 1\}^n$ $n-$dimenzionalni vektori. Ova reprezentacija se naziva algebarskom normalnom formom funkcije $f(x_1, x_2, \ldots, x_n)$.

- Za datu Bulovu funkciju $f$ i njenu algebarsku normalnu formu datu sa (2.7) definiše se algebarski stepen funkcije $f$ sa

$$\deg(f) = \max_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} \{d \mid d = \alpha_1 + \alpha_2 + \ldots + \alpha_n\}.$$

Numerička karakteristika algebarskog stepena Bulove funkcije u određenoj je vezi sa korelacionom imunošću konstrukcija u kojima se data funkcija primenjuje.

- Bulova funkcija $f$ je balansirana ako važi

$$\begin{aligned} &|\{(x_1, x_2, \ldots, x_n) \mid f(x_1, x_2, \ldots, x_n) = 0\}| \\ &\qquad = |\{(x_1, x_2, \ldots, x_n) \mid f(x_1, x_2, \ldots, x_n) = 1\}| \end{aligned}$$

za $(x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$ gde $|A|$ označava broj elemenata skupa $A$. Balansiranost je važna osobina u kriptografskim konstrukcijama jer njeno narušavanje otvara mogućnosti za napade statističkog tipa na konstrukcije u kojima se koriste nebalansirane funkcije.

- Skup svih linearnih Bulovih funkcija od $n$ promenljivih označimo sa $\mathcal{L}_n$ a skup svih Bulovih funkcija sa $\mathcal{B}_n$. Nelinearna složenost Bulove funkcije $f \in \mathcal{B}_n$ definiše se sa

$$nl(f) = \min_{l \in \mathcal{L}_n} d_H(f, l)$$

gde $d_H$ označava Hemingovo rastojanje. Nelinearna složenost ukazuje na mogućnost aproksimacije date funkcije linearnim i afinim Bulovim funkcijama. Izborom optimalne vrednosti ovog parametra pri sintezi sekvencijalnih kriptografskih algoritama onemogućavaju se napadi u kojima se Bulove funkcije aproksimiraju linearnim funkcijama i cela konstrukcija bitno uprošćava.

- Bulova funkcija $f$ je korelaciono imuna reda $k$ ako je $f(x_1, x_2, \ldots, x_n)$ statistički nezavisno od proizvoljno odabranih $k$ promenljivih $x_{i_1}, x_{i_2}, \ldots x_{i_k}$. Korelaciona imunost ukazuje na otpornost funkcije na korelacione napade.

- Ako za datu Bulovu funkciju $f(x_1, x_2, \ldots, x_n) \in \mathcal{B}_n$ postoji funkcija $g\big(x_1, x_2, \ldots, x_n\big) \in \mathcal{B}_n$ takva da je

$$f(x_1, x_2, \ldots, x_n) \cdot g(x_1, x_2, \ldots, x_n) = 0$$

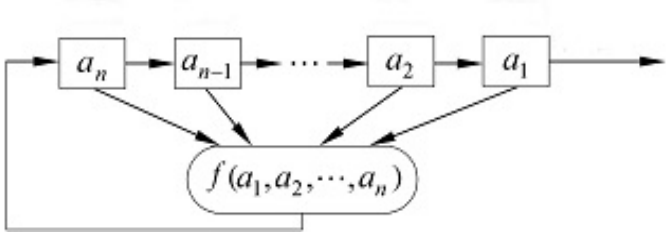
  tada se $g(x_1, x_2, \ldots, x_n)$ naziva anihilatorom za $f(x_1, x_2, \ldots, x_n)$. Označimo sa $\mathcal{A}(h), \quad h \in \mathcal{B}_n$ skup anihilatora funkcije $h$. Algebarska imunost date funkcije $f(x_1, x_2, \ldots, x_n) \in \mathcal{B}_n$ definiše se sa

$$AI(f) = \min_{g \in \mathcal{A}(f) \bigcup \mathcal{A}(1 \oplus f)} \{d(g)\}$$

  Algebarska imunost je pokazatelj otpornosti funkcije na algebarske napade.

Potpuniji i detaljniji prikaz kriptografskih osobina Bulovih funkcija može se naći u [41–44].

Osobine Bulovih funkcija se analiziraju kako bi se njihovom primenom u sintezi kriptografskih algoritama postigla maksimalna bezbednost i otpornost kriptografskog algoritma na kriptoanalitičke napade. Na žalost, ispostavlja se da nije retka situacija da su neki od tih zahteva međusobno protivrečni, kao na primer zahtevi u odnosu na korelacionu imunost i algebarski stepen. U takvim situacijama na kreatoru je da odabere optimalne vrednosti parametara u procesu sinteze kriptografskog algoritma kako bi se dobila bezbednosno pouzdana konstrukcija.




Slika 2.10: Pomerački registar sa povratnom spregom, [15]

#### 2.3.1.2 Pomerački registri sa povratnom spregom

Pored Bulovih funkcija jedan od često primenjivanih gradivnih elemenata u sintezi kriptografskih algoritama su pomerački registri sa povratnom spregom.

Odlikuju se efikasnom implementacijom i radom i u softverskoj i u hardverskoj realizaciji. Grafički prikaz pomeračkog registra sa povratnom spregom dat je na slici 2.10. Neke od njihovih osnovnih osobina date su u nastavku.

Definišimo sada pomeračke registre sa povratnom spregom.

Neka je dato konačno polje $\mathbb{F}_q$. Za niz elemenata $a_i \in \mathbb{F}_q$, $i = 0, 1, 2, .....$ kažemo da je generisan pomeračkim registrom dužine $n$ sa povratnom spregom primenom funkcije $f : \underbrace{\mathbb{F}_q \times \mathbb{F}_q \times \ldots \times \mathbb{F}_q}_{n} \longrightarrow \mathbb{F}_q$ ako važi

$$\begin{aligned} a_i &\in \mathbb{F}_q,\ i = 0, 1, ..., n-1, \\ a_{n+k} &= f\left(a_{n+k-1}, a_{n+k-2}, \ldots, a_k\right), \quad k = 0, 1, \ldots \end{aligned} \tag{2.8}$$

gde su $a_i,\ i = 0, 1, ..., n-1$, zadate početne vrednosti i vektor $(a_0, a_1, \ldots, a_{n-1})$ se naziva početnim stanjem pomeračkog registra. Niz $\{a_i\}_{i=0}^{\infty}$ generisan u skladu sa jednačinom (2.8) zovemo nizom generisanim pomeračkim registrom dužine $n$. Naziv za ovaj tip nizova potiče iz inženjerske prakse, odnosno načina na koji se ovaj tip nizova izračunava u procesnim uređajima. Prikaz jednog takta pri računanju elementa ovog niza dat je na slici 2.10. Ova tehnika računanja elemenata niza $\{a_i\}_{i=0}^{\infty}$ je izuzetno efikasna jer koristi samo $n$ memorijskih ćelija za argumente i procesni element za funkciju $f$.

Iz načina na koji je niz $\{a_i\}_{i=0}^{\infty}$ definisan, lako se zaključuje da je za svaku funkciju $f$ on periodičan ali dužina perioda zavisi od izabrane funkcije. U zavisnosti od osobina funkcije $f$ pomerački registri se dele na

1. Linearne pomeračke registre sa povratnom spregom, kada je $f$ linearna funkcija nad $\mathbb{F}_q$,

2. Nelinearne pomeračke registre sa povratnom spregom, kada je $f$ nelinearna funkcija nad $\mathbb{F}_q$.

**2.3.1.2.1 Linearni pomerački registri sa povratnom spregom** Linearni pomerački registri sa povratnom spregom (Linear Feedback Shift Register - LFSR) se često koriste za sintezu sekvencijalnih kriptografskih algoritama. Više je razloga za to. Pre svega njihova struktura i funkcionalnost se lako realizuje u hardveru, nizovi koje generišu imaju neke kriptografski važne osobine i njihov teorijski model je pogodan za algebarsku analizu koja omogućava teorijsko potvrđivanje osobina

sekvencijalnih kriptografskih generatora u kojima se koriste. Linearni pomerački registri se dobijaju kada je u (2.8) funkcija $f$ oblika

$$f(x_1, x_2, \ldots, x_n) = c_1 \cdot x_1 + c_2 \cdot x_2 + \ldots + c_n \cdot x_n, \qquad (2.9)$$
$$c_i \in \mathbb{F}_q,\ i = 1, 2, ..., n,$$

U tom slučaju pomerački registar se naziva linearnim pomeračkim registrom dužine $n$ a jednačine kojima se definiše niz $\{a_i\}_{i=0}^{\infty}$ su date sa

$$a_i \in \mathbb{F}_q,\ i = 0, 1, ..., n-1, \qquad (2.10)$$
$$a_{n+k} = c_1 \cdot a_{n+k-1} + c_2 \cdot a_{n+k-2} + \ldots + c_n \cdot a_k, \quad k = 0, 1, \ldots$$

gde su + i $\cdot$ operacije sabiranja i množenja u polju $\mathbb{F}_q$. Svakom linearnom pomeračkom registru se može pridružiti polinom $p(x) = \sum_{i=0}^{n} c_i \cdot x^i, \quad c_0 = 1$ koji se naziva polinomom povratne sprege linearnog pomeračkog registra. Od osobina polinoma povratne sprege zavise i osobine niza $\{a_i\}_{i=0}^{\infty}$. Detaljna teorija sa definicijama, karakterizacijama i oblastima primene može se naći u [45].

U sintezi sekvencijalnih kriptografskih algoritama najčešće se primenjuju linearni pomerački registri nad konačnim poljem $\mathbb{F}_2$.

Neka je dat linearni pomerački registar dužine $n$ sa polinomom povratne sprege $p(x)$. Sledeće osobine linearnih pomeračkih registara sa kriptografskog stanovišta su važne:

- Niz $\{a_i\}_{i=0}^{\infty}$ je jedinstveno određen početnim stanjem i polinomom povratne sprege $p(x)$,
- Ako je polinomom povratne sprege $p(x)$ primitivan u $\mathbb{F}_2[x]$ tada je period izlaznog niza jednak $2^n - 1$ za svako od $2^n - 1$ mogućih početnih stanja. Jedino početno stanje $\overbrace{(0, 0, ..., 0)}^{n}$ daje niz sa periodom 1, nula niz. Nizovi sa periodom $2^n - 1$ nazivaju se nizovima sa maksimalnim periodom, $m-$nizovi.
- Ako je $k$ prirodan broj tako da je $1 \leq k \leq n$ i neka je $a_{i+1}, a_{i+2}, \ldots, a_{i+2^n+k-2}$ podniz niza $\{a_i\}_{i=0}^{\infty}$ dužine $2^n + k - 2$ tada se svaka sekvenca binarnih simbola dužine $k$ javlja u izabranom podnizu tačno $2^{n-k}$ puta.
- Na periodu niza $\{a_i\}_{i=0}^{\infty}$, podniz dužine $2^n - 1$, broj jedinica i nula se razlikuje najviše za 1.

- Pod serijama podrazumevamo nizove uzastopnih jednakih simbola. Nizove uzastopnih jedinica nazivamo blokovi a nizove uzastopnih nula nazivamo razmacima. U tom slučaju jedna polovina serija ima dužinu jedan, četvrtina dužinu dva, osmina dužinu tri i tako sve dok je broj serija određene dužine veći od jedan. Broj korespondentnih blokova i razmaka je približno jednak.

- Autokorelaciona funkcija uzima dve vrednosti

$$(2^n-1)\,C\,(t)=\sum_{i=0}^{2^n-2}(2a_i-1)\cdot(2a_{i+t}-1)=\begin{cases}2^n-1 & t=0\\ \\ k & 1\leq t\leq 2^n-1\end{cases}$$

  za neki broj $k$.

Pored ovih kriptografski poželjnih osobina, linearni pomerački registri imaju i jednu kriptografsku slabost koja je indukovana njihovom linearnošću. Pokazuje se da je dovoljno poznavanje $2n$ uzastopnih elemenata izlaznog niza za rekonstrukciju početnog stanja i polinoma povratne sprege a potom i čitavog niza $\{a_i\}_{i=0}^{\infty}$. Iako na prvi pogled izgleda da ova osobina u potpunosti diskredituje linearne pomeračke registre za primenu u sintezi kriptografskih algoritama to nije tako. Postoje tehnike upotrebe linearnih pomeračkih registara u sintezi sekvencijalnih kriptografskih algoritama kojima se ova slabost može prevazići a da njihove dobre kriptografske karakteristike doprinose snazi kriptografskog algoritma koji se kreira. Jedan od očiglednih načina za prevazilaženje ovog problema je upotreba nelinearnih pomeračkih registara sa povratnom spregom.

**2.3.1.2.2 Nelinearni pomerački registri sa povratnom spregom** Nelinearni pomerački registri se definišu sistemom jednačina (2.8) i grafički su prikazani na slici 2.10 uz uslov da funkcija $f$ nije linearna. Standardni alati u predstavljanju i analizi nelinearnih pomeračkih registara su teorija konačnih automata, teorija grafova i teorija Bulovih funkcija. I u ovom slučaju kriptografska praksa se najčešće oslanja na razmatranja u konačnom polju $\mathbb{F}_2$.

Kako su nelinearni pomerački registri po svojoj suštini konačni automati to su njima generisani nizovi nužno periodični. Period može biti najviše $2^n$ koliko ukupno ima binarnih vektora dužine $n$. Nizovi generisani nelinearnim pomeračkim registrima sa povratnom spregom koji imaju period $2^n$ nazivaju se de Bruijnovi nizovi. Za de Bruijn-ove nizove važi:

- Period im je jednak $2^n$
- Ako je $k$ prirodan broj tako da je $1 \leq k \leq n$ i neka je $a_{i+1}, a_{i+2}, \ldots, a_{i+2^n+k-1}$ podniz niza $\{a_i\}_{i=0}^{\infty}$ dužine $2^n + k - 1$ tada se svaka sekvenca simbola dužine $k$ javlja u izabranom podnizu tačno $2^{n-k}$ puta.

Nelinearni pomerački registri sa povratnom spregom nisu izučavani u meri u kojoj je to slučaj sa njihovim linearnim parnjacima. Razlozi se pre svega mogu pronaći u složenosti problema, opštosti funkcija koje se razmatraju i shodno tome nedostatku metoda i tehnika za uniforman tretman tako opštih klasa funkcija. Dodatni rezultati mogu se naći u [46], [47].

#### 2.3.1.3 ARX konstrukcije

Ovaj tip sinteze sekvencijalnih kriptografskih algoritama namenjen je sintezi sekvencijalnih kriptografskih algoritama koji se realizuju u hardveru što se vidi po izboru operacija koje se u konstrukcijama ovog tipa koriste.

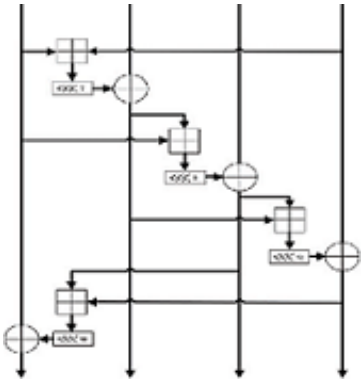
U ovim konstrukcijama od operacija nad podacima koristi se samo sledeće tri operacije:

- sabiranja po modulu $2^n$, označava se sa $\boxplus$,
- operacije cikličkog pomeranja u levo, označava se sa $\lll$ i
- sabiranja po modulu 2 koje nazivamo ekskluzivna disjunkcija ($XOR$) i označava se sa $\oplus$.

Operacijama cikličkog pomeranja u levo i ekskluzivne disjunkcije realizuje se principi difuzije a sabiranjem po modulu $2^n$ se postiže nelinearnost transformacije i realizuje princip konfuzije. Principi konfuzije i difuzije opisani su na strani 11. Ovaj tip konstrukcije prikazan je na slici 2.11, deo runde u algoritmu SALSA20.

Primeri kriptografskih algoritama dizajniranih na ovom principu su Salsa 20, [38], i Chacha, [49].

Za kriptografske algoritme ovog tipa karakteristično je da su njihove implementacije softverski kompaktne i vrlo efikasne u izvršavanju što pospešuje interesovanje kriptografske zajednice za ovakav tip kriptografske sinteze.



Slika 2.11: Deo transformacije u kriptografskom algoritmu Salsa 20

### 2.3.2 Primeri sprezanja osnovnih gradivnih struktura u sintezi sekvencijalnih kriptografskih algoritama

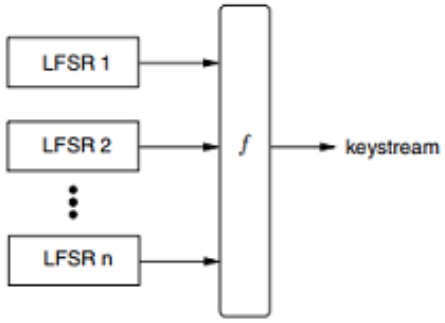
Sinteza sekvencijalnih kriptografskih algoritama zasnovana je na upotrebi jednog ili više prethodno opisanih tipova gradivnih elemenata. Cilj sinteze sekvencijalnih kriptografskih algoritama je kreiranje kriptografski kvalitetnih sekvencijalnih algoritama. Osnovni kriterijumi kriptografskog kvaliteta za sekvencijalne kriptografske algoritme su:

1. dobre statističke osobine
2. veliki period
3. velika linearna složenost.

Mora se naglasiti da ispunjenost ovih kriterijuma predstavlja samo neophodne pokazatelje kriptografskog kvaliteta ali ne i dovoljne. U odeljku 2.3.1.2.1 je konstatovano da linearni pomerački registri sa povratnom spregom imaju veliki period i dobre statističke osobine ali da samostalno nisu primenljivi u sintezi sekvencijalnih kriptografskih algoritama. U ovom delu ćemo prikazati neke načine sprezanja osnovnih gradivnih struktura sekvencijalnih kriptografskih algoritama i njihove bezbednosne karakteristike. Termin "takt" u ovom delu treba shvatiti kao što je navedeno delu 2.2.1.

#### 2.3.2.1 Nelinearni kombinacioni generator bez memorije

Metod sprezanja osnovnih gradivnih struktura sekvencijalnih kriptografskih algoritama u kojem se koristi nekoliko linearnih pomeračkih registara sa povratnom spregom i nelinearna Bulova funkcija $f$ naziva se kombinacioni generator. Ovaj vid sprezanja onemogućava prenos karakteristike linearnosti linearnih pomeračkih registara na izlazni niz. Grafički prikaz ovog tipa generatora dat je na slici 2.12.

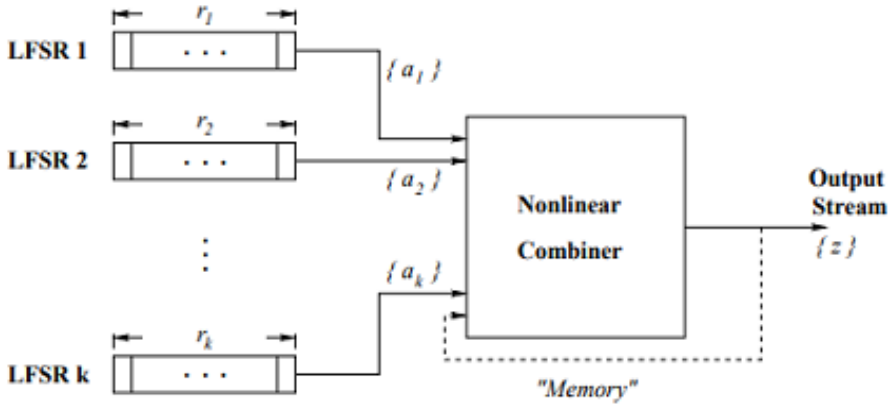



Slika 2.12: Kombinacioni sekvencijalni kriptografski generator, [15]

Uz dobro odabranu funkciju $f$ ovaj tip generatora ima dobre statističke karakteristike i veliku linearnu složenost. Sa druge strane, konstrukcija je podložna korelacionim napadima, [50], [51]. Za odabranu funkciju $f$ od $n$ promenljivih sa algebarskim stepenom $d$ i korelacionom imunošću $m$ važi $d + m \leq n$, [52]. Za kriptografske algoritme je poželjno da oba parametra imaju što veću vrednost što očigledno nije moguće. Zbog relacije $d+m \leq n$ jasno je da se povećavanjem jednog parametra drugi smanjuje. Iz tih razloga se pri sintezi ovog tipa generatora mora voditi računa o pravilnom izboru funkcije $f$ u svetlu vrednosti brojeva $n$, $m$ i $d$.

#### 2.3.2.2 Nelinearni kombinacioni generator sa memorijom

Nelinearni kombinacioni generator sa memorijom je generalizacija kombinacionih generatora koji poseduje dobra kriptološka svojstva i koristi se i u teoriji i u praksi. Tako na primer ova konstrukcija se koristi u kriptografskom algoritmu $E0$, [21], koji je namenjen za zaštitu poruka u bežičnim i Bluetooth komunikacionim mrežama. Detaljan i potpun prikaz ovog tipa sprezanja sa bezbednosnom analizom ove konstrukcije može se naći u [53].




Slika 2.13: Nelinearni kombajner generator sa memorijom

#### 2.3.2.3 Neuniformno taktovani linearni pomerački registri

U konstrukcijama koje se odnose na nelinearne kombinacione generatore linearni pomerački registri se taktuju sinhrono a linearnost koju oni inherentno poseduju i njen transfer u izlazni niz se suzbija primenom nelinearne Bulove funkcije $f$. Drugi pristup koji omogućava konstrukcije sekvencijalnih kriptografskih algoritama upotrebom linearnih pomeračkih registara i suzbijanje linearnosti izlaznog niza sastoji se u ideji da se linearni pomerački registri koji učestvuju u konstrukciji ne taktuju sinhrono već da jedan deo njih upravlja taktovanjem nekih od preostalih linearnih pomeračkih registara. Sledeće dve konstrukcije sa neuniformno taktovanim linearnim pomeračkim registrima se najčešće koriste u praksi.

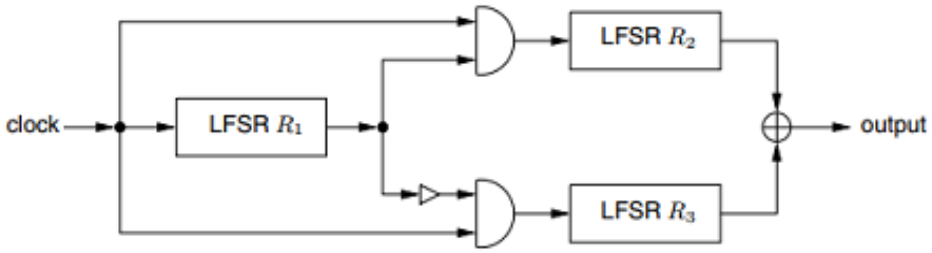
**2.3.2.3.1 Generator alternirajućeg taktovanja** Ovu tehniku supresije prenosa karakteristika linearnosti linearnih pomeračkih registara na izlazni niz predložio je Günther u [54]. Konstrukcija se sastoji od tri linearna pomeračka registra, označimo ih sa $R_1, R_2$ i $R_3$ a njihove izlazne nizove sa $\{r_i^1\}_{i=0}^{\infty}$, $\{r_i^2\}_{i=0}^{\infty}$, $\{r_i^3\}_{i=0}^{\infty}$ respektivno. Izlazni niz ovog generatora označićemo sa $\{z_i\}_{i=0}^{\infty}$. Dobijanje elemenata izlaznog niza opisuje se sledećim sistemom jednačina:

$$k(i) = \left(\sum_{l=0}^{i} r_i^1\right) - 1$$
$$z_i = r_k^3 \oplus r_{k-i-1}^2$$
$$r_{-1}^2 = r_{-1}^3 = 0$$
$$i = 0, 1, ...$$

Deskriptivno govoreći generisanje izlaznog elementa se odvija na sledeći način.

Taktuje se registar $R_1$ i ako je njegova izlazna vrednost jedan taktuje se registar $R_2$. Izlazna vrednost registra $R_2$ se sabere po modulu dva sa izlaznom vrednošću registra $R_3$ iz prethodnog takta i taj zbir je izlazna vrednost konstrukcije u tekućem taktu. Ako je izlazna vrednost registra $R_1$ nula taktuje se registar $R_3$. Izlazna vrednost registra $R_3$ se sabere po modulu dva sa izlaznom vrednošću registra $R_2$ iz prethodnog takta i taj zbir je izlazna vrednost konstrukcije u tekućem taktu.

Grafički prikaz generatora alternirajućeg taktovanja dat je na slici 2.14

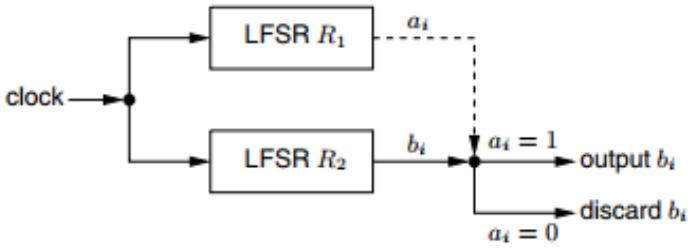



Slika 2.14: Grafički prikaz generatora alternirajućeg takta, [15]

U pogledu kriptografskih svojstava generator alternirajućeg takta ima veoma dobre karakteristike.

Pretpostavimo da je $R_1$ dužine $n_1$ i da generiše de Brujinov niz sa periodom $2^{n_1}$. Neka su polinomi povratne sprege registara $R_2, R_3$ primitivni a za njihove dužine $n_2, n_3$ važi $\gcd(n_2, n_3) = 1$. Tada za izlazni $\{z_i\}_{i=0}^{\infty}$ niz važi, [54]:

- Izlazni niz $\{z_i\}_{i=0}^{\infty}$ ima period $2^{n_1} \cdot (2^{n_2} - 1) \cdot (2^{n_2} - 1)$
- Linearna složenost izlaznog niza $\{z_i\}_{i=0}^{\infty}$, označena sa $L(z)$ je ograničena sa
$$(n_2 + n_3) \cdot 2^{n_1 - 1} < L(z) \leq (n_2 + n_3) \cdot 2^{n_1}$$
- Ako se polinomi povratne sprege biraju na slučajan način iz odgovarajućih skupova primitivnih polinoma u $\mathbb{F}_2[x]$ i neka je $L$ proizvoljan niz binarnih simbola dužine $l$ gde je $l \leq \min(n_1, n_2)$. Tada je verovatnoća da proizvoljna niska izlaznih simbola dužine $l$ bude jednaka sa $L$ data sa
$$\frac{1}{2l} + O\left(\frac{t}{2^{n_2 - l}}\right) + O\left(\frac{t}{2^{n_3 - l}}\right)$$
Slobodnije rečeno raspodele verovatnoća za $l-$ torke su uniformne.




Slika 2.15: Grafički prikaz generatora neuniformne decimacije, [15]

Za generatore alternirajućeg taktovanja nije poznat efikasan napad koji bi ih kompromitovao kada je $\min(n_1, n_2, n_3) \geq 128$.

**2.3.2.3.2 Generator neuniformne decimacije** Generator neuniformne decimacije je konstrukcija koja se u literaturi pojavila 1993 u radu Kopersmita, Kravčuka i Mansura [55]. Generator se sastoji od dva linearna pomeračka registra $R_1$ i $R_2$. Izlazni niz se generiše na sledeći način.

Registri $R_1$ i $R_2$ se taktuju i ako je izlaz iz registra $R_1$ jednak jedan tada se kao izlazni element generiše izlaz iz registra $R_2$. Ako je izlaz iz registra $R_1$ jednak nula tada se izlaz iz registra $R_2$ odbacuje, generator ne proizvodi izlaz već se prelazi na novi takt. Grafički je rad generatora neuniformne decimacije prikazan na slici 2.15

U pogledu kriptografskih svojstava generator neuniformne decimacije ima veoma dobre karakteristike.

Neka su polinomi povratne sprege registara $R_1, R_2$ primitivni a njihove dužine $n_1, n_2$ redom. Tada za izlazni niz $\{z_i\}_{i=0}^{\infty}$ važi, [55]:

- Ako je $\gcd(n_1, n_2) = 1$ tada izlazni niz $\{z_i\}_{i=0}^{\infty}$ ima period $2^{n_1-1} \cdot (2^{n_2} - 1)$
- Linearna složenost izlaznog niza $\{z_i\}_{i=0}^{\infty}$, označena sa $L(z)$ je ograničena sa
$$n_2 \cdot 2^{n_1-2} < L(z) \leq n_2 \cdot 2^{n_1-1}$$
- Ako se polinomi povratne sprege biraju na slučajan način iz odgovarajućih skupova primitivnih polinoma u polju $\mathbb{F}_2$ tada je za proizvoljan niz binarnih simbola $L$ dužine $l$ verovatnoća da proizvoljna niska izlaznih simbola bude jednaka sa $L$ data sa
$$\frac{1}{2^l} + O\left(\frac{l}{2^{n_2}}\right)$$
Slobodnije rečeno raspodele verovatnoća za $l-$ torke su uniformne.

## 2.4 Modeli bezbednosti kriptografskih algoritama

Kriptologija je nastala iz potrebe da se razmenjuju informacije koje će biti dostupne samo onima kojima su namenjene. Prirodna ideja povodom tog problema je bila da se poruke prenose u formi u kojoj njen sadržaj neće biti dostupan nikome osim onom kome je poruka namenjena. U prvo vreme procedura transformacije poruke u željenu formu, šifrovanje, i parametri koji u transformaciji učestvuju, ključ, smatrani su tajnom koju dele pošiljalac i primalac. Dostupnost informacija koju poruka nosi zasnivala se na poznavanju primenjene transformacije i kriptografskog ključa. Intuitivno, takav pristup deluje ispravno jer ako napadač ne zna ništa o sistemu šifrovanja onda nema nikakve praktične šanse da dođe do sadržaja poruke. Na prvi pogled ovakav pristup pruža visok nivo sigurnosti ali to nije tako.

Strane koje koriste tajan šifarski sistem nemaju nikakvu potvrdu njegovog kvaliteta. Sigurnost svoje komunikacije oni zasnivaju na tajnosti upotrebljenog šifarskog sistema ali nemaju načina da se u njegovu tajnost uvere. Moguće je da neko ko je zainteresovan za informacije o upotrebljenom šifarskom sistemu do njih dođe a da strane koje ga koriste o tome nemaju indikacija. U tom slučaju sigurnost komunikacije zavisi od kvaliteta primenjene transformacije o čemu potvrdu komunikacione strane imaju samo na nivou svoga znanja.

Prethodni scenario je često dovodio do narušavanja sigurnosti komunikacija i zbog toga se sa razmišljanjima krenulo u drugom smeru.

Auguste Kerhofs je krajem 19. veka u svojim delima [56], [57] gde se bavio definisanjem dizajnerskih principa za vojne i državne kriptografske algoritme promovisao sasvim suprotno gledište. Taj princip, koji se danas naziva Kerhofsov princip, glasi:

> "*Metode šifrovanja nije neophodno držati tajnim i moraju biti takve da pad u ruke neprijatelja ne ugrožava funkcionisanje komunikacija.*"

Ovo znači da komunikacioni, odnosno šifarski sistem treba da bude tako dizajniran i realizovan da kada je napadaču poznato sve osim primenjenog kriptografskog ključa zaštićeni podaci mu ostaju nedostupni. Nekoliko činjenica i danas govori u prilog Kerhofsovog principa.

U sistemima gde je relativno veliki broj korisnika, velike kompanije, državna uprava, ministarstva..., neuporedivo je lakše imati kontrolu nad tajnošću kripto-

grafskog ključa koji je relativno kratak podatak nego nad relativno velikim šifarskim sistemom u kojem svaki komunikacioni par koristi drugačiju šifarsku transformaciju. Efikasno održavanje i upravljanje takvim komunikacionim šifarskim sistemom je gotovo nemoguće.

U komunikacionom sistemu se može desiti da i pored kvalitetnog algoritma šifrovanja neki primenjeni kriptografski ključ bude kompromitovan i poruke zaštićene njime budu poznate napadaču. U sistemima dizajniranim po Kerhofsovom principu tada je neophodno samo korisnicima dostaviti druge kriptografske ključeve što je neuporedivo manji posao od menjanja algoritama šifrovanja i njima pripadajućih ključeva što bi se moralo učiniti u sistemima koji se oslanjaju na tajnost kriptografskog algoritma i ključeva. Generisanje kriptografskih ključeva je posao daleko manjeg obima nego kompletna zamena algoritama šifrovanja.

U skladu sa proklamovanim principom poželjno je po sintezi kriptografskog algoritma a pre njegove upotrebe javno obznaniti njegov opis. Kriptografski algoritmi su uvek intrigirali javnost i akademsku zajednicu pa je opravdana pretpostavka da bi ih njegovo prisustvo u javnosti potaklo na analizu njegovih osobina. Takva masovna analiza, u koju bi svakako bili uključeni kompetentni pojedinci i ustanove, sa velikom verovatnoćom bi detektovala njegove slabosti u slučaju da postoje. U slučaju da u nekom razumnom roku, recimo nekoliko godina, od prisustva algoritma u javnosti slabosti ne budu detektovane kriptografski algoritam bi se mogao smatrati dovoljno kvalitetnim za upotrebu. Ovakva proceduralna praksa otvara vrata ka standardizaciji kriptografskih rešenja što se već odigralo na primeru algoritma AES, [58]. Standardizacija u oblasti kriptografskih algoritama ima pozitivan uticaj na razvoj sigurnosti u informaciono-komunikacionim mrežama jer pospešuje bezbednosnu kompatibilnost između različitih korisnika i upotrebu pouzdanih kriptografskih algoritama.

Kerhofsov princip nam daje savet o jednom aspektu sinteze kriptografskih algoritama ali nam ne daje kriterijume za ocenu kada se kriptografski algoritam može smatrati bezbednim i šta je to bezbednost kriptografskog algoritma. Ovo pitanje se može učiniti nepotrebnim jer svako od nas ima intuitivan osećaj te vrste bezbednosti. Jedna od verbalizacija te intuicije bi mogla da glasi:

> "*Bez obzira na prirodu i sadržaj informacija koje napadač ima a ne uključuju primenjeni kriptografski ključ, posedovanje i poznavanje šifrata ni na koji način ne uvećava napadačevu količinu informacija o otvorenom tekstu iz kojeg je šifrat nastao.*"

Da bi se na osnovu ove intuitivne definicije bezbednosti mogli donositi zaključci o kvalitetu i snazi kriptografskog algoritma mora se kreirati okruženje i pristup koji omogućava izvođenje formalnih zaključaka. Prema tome neophodno je definisati pojmove šifarskog sistema, napadača na sistem i njegove ciljeve.

Šifarski sistem se karakteriše skupom poruka koje štiti, algoritmom za šifrovanje, algoritmom za dešifrovanje i skupom kriptografskih ključeva. Označimo sa $\mathcal{K}, \mathcal{M}, \mathcal{C}$ prostor kriptografskih ključeva, prostor otvorenih poruka i prostor šifrata respektivno. Usvojićemo sledeću definiciju:

**Definicija 1** *Šifarski sistem nad prostorom poruka* $\mathcal{M}$, $|\mathcal{M}| > 1$, *je uređena trojka* $(G, E, D)$ *gde je*

- *Funkcija izbora ključeva* $G : \mathbb{N} \longrightarrow \mathcal{K}$ *slučajna promenljiva data sa* $G(n) = k$, *i* $|k| = n$. *Raspodela verovatnoća* $P(G(n) = k)$ *određena je kontekstom.*
- *Algoritam šifrovanja je preslikavanje* $E : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$ *dato sa* $E(k, m) = E_k(m) = c$
- *Algoritam dešifrovanja je preslikavanje* $D : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$ *dato sa* $D(k, c) = D_k(c) = m$

Da bi se moglo govoriti o otpornosti kriptografskog algoritma na napade i formalno izvoditi zaključci o tome mora se pre svega definisati pojam napada na kriptografski algoritam. Napadač, odnosno napad, na kriptografski algoritam karakteriše se napadačevim sposobnostima i njegovim ciljem. Napadačeve sposobnosti sadrže dve komponente

1. Napadačevu računarsku snagu koja se karakteriše klasom algoritama koje napadač može efikasno da izvršava u smislu teorije složenosti računarskih algoritama.
2. Tip i količinu informacija koje napadač poseduje. Obično se razmatraju sledeći slučajevi:
   - **Poznavanje šifrata** (Ciphertext only attack - CPA) podrazumeva da napadač na neki način uspeva da dođe do određene količine šifrata i njegovom analizom pokušava da dođe do informacija o porukama ili primenjenom kriptografskom ključu.

- **Poznavanje određenog broja parova (poruka, šifrat) šifrovanih istim ključem** (Known plaintext attack - KPA). Koristeći podatke koje ima napadač pokušava da dođe do informacija o nekim drugim šifrovanim porukama.
- **Poznavanje šifrata za izabrane poruke** (Chosen plaintext attack-CPA). U ovom slušaju napadač može da izabere poruke čije šifrate nekako dobija i potom pokušava da dođe do informacija o nekim drugim šifrovanim porukama.
- **Poznavanje nekih informacija o odabranim šifratima** ali ne i njihov dešifrovani oblik, (Chosen ciphertext attack -CCA)

Prilikom određenja napada nikakve pretpostavke se ne prave o napadačevoj strategiji odnosno načinu upotrebe informacija kojima raspolaže i algoritmu koji će koristiti prilikom napada.

Određenjem kriptografskog sistema i napadača omogućeno je da se o napadima na kriptografske algoritme može formalno zaključivati.

### 2.4.1 Informaciono-teoretski pristup bezbednosti kriptografskih algoritama

Ustanovljavanjem okruženja u kojem možemo formalno zaključivati o kriptografskim algoritmima prirodno je postaviti pitanje da li postoji i kako izgleda kriptografski algoritam koji je otporan na svaku vrstu napada. Imajući u vidu da je usvojeni Kerhofsov princip smatramo da su napadaču poznate sve informacije o sistemu osim primenjenog kriptografskog ključa. U skladu sa nekom raspodelom verovatnoća odabrana je poruka $m$ iz skupa $\mathcal{M}$ i neka je njen šifrat $c$. Napadač je u stanju da nadgledanjem komunikacija dođe u posed šifrata $c$. Ako je posmatrani sistem apsolutno siguran onda je prirodno da napadač iz šifrata nije u stanju da izvuče nikakvu informaciju o poruci koju šifrat predstavlja. Drugim rečima, aposteriorna verovatnoća po prijemu šifrata $c$ da je poslata neka poruka $m \in \mathcal{M}$ je jednaka apriornoj verovatnoći da je za slanje odabrana baš poruka $m$. Odavde sledi:

**Definicija 2** *Šifarski sistem* $(G, E, D)$ *u prostoru poruka* $\mathcal{M}$ *je apsolutno siguran ako za svaku funkciju raspodele nad* $M$*, svaku poruku* $m \in \mathcal{M}$ *i svaki šifrat* $c \in \mathcal{C}$

*za koji je* $P(C = c) > 0$ *važi*

$$P(M = m \,|\, C = c) = P(M = m) \tag{2.11}$$

Ovde treba uočiti da je uslov $P(C = c) > 0$ u definiciji 2 tehničke prirode zbog definicije uslovne verovatnoće.

Dokažimo sada sledeću teoremu.

**Teorema 3** *Šifarski sistem* $(G, E, D)$ *u prostoru poruka* $\mathcal{M}$ *je apsolutno siguran ako i samo*

$$P(E_K(m_1) = c) = P(E_K(m_2) = c) \tag{2.12}$$

*za svake dve poruke* $m_1, m_2 \in \mathcal{M}$ *i svaki šifrat* $c \in \mathcal{C}$.

**Dokaz.** Neka $K, M$ i $C$ slučajne promenljive čije su vrednosti ključevi, poruke i šifrati redom i neka su njihove funkcije raspodele proizvoljne. Tada je za svako $m \in \mathcal{M}$ za koje je $P(M = m) > 0$ i svako $c \in \mathcal{C}$ ispunjeno

$$\begin{aligned} P(C = c \,|\, M = m) &= P(E_K(M) = c \,|\, M = m) \\ &= P(E_K(m) = c \,|\, M = m) \\ &= P(E_K(m) = c) \end{aligned} \tag{2.13}$$

u (2.13) prva jednakost je ispunjena po definicija slučajne promenljive $C$. Druga jednakost je ispunjena zbog uslovne verovatnoće po $M = m$ a treća jednakost je ispunjena jer su $K$ i $M$ nezavisne slučajne promenljive. Iz definicije uslovne verovatnoće imamo da je za svako $P(C = c) > 0$ ispunjeno

$$P(M = m \,|\, C = c) \cdot P(C = c) = P(C = c \,|M = m) \cdot P(M = m) \tag{2.14}$$

Dokažimo sada da je uslov potreban.
Kako je sistem apsolutno siguran koristeći definiciju 2 i jednačinu (2.14) dobijamo da je

$$P(C = c \,|M = m) = P(C = c) \tag{2.15}$$

Kako su $m, c$ u jednakosti (2.15) proizvoljni to za proizvoljno $m_1$ imamo

$$\begin{aligned} P(C = c) &= P(C = c \,|M = m_1) \\ &= P(E_K(M) = c \,|M = m_1) \\ &= P(E_K(m_1) = c \,|M = m_1) \\ &= P(E_K(m_1) = c) \end{aligned} \tag{2.16}$$

Uzimajući sad proizvoljno $m_2$ na isti način dobijamo

$$P(C = c) = P(E_K(m_2) = c) \tag{2.17}$$

Koristeći sada jednakosti (2.16) i (2.17) dobijamo

$$P(E_k(m_1) = c) = P(E_k(m_2) = c)$$

što je i trebalo dokazati.
Pokažimo sada da je uslov dovoljan.
Neka važi jednakost (2.12) dokažimo da je sistem apsolutno siguran.
Neka je nad skupom poruka data proizvoljna funkcija raspodele. Neka je $m \in \mathcal{M}$ proizvoljna poruka i $c \in C$ proizvoljan šifrat za koji važi $P(C = c) > 0$.
Neka je $P(M = m) = 0$
Tada iz jednačine (2.12) i iz uslova $P(C = c) > 0$ direktno dobijamo

$$P(M = m \,|\, C = c) = 0$$

što direktno daje

$$P(M = m \,|\, C = c) = P(M = m)$$

čime je tvrdnja u ovom slučaju dokazana.
Neka je sada $P(M = m) > 0$.
Za proizvoljno $c \in C$ stavimo $p_c \overset{def}{=} P(E_K(m) = c)$.
Vrednost $p_c$ je dobro definisana jer je $P(C = c) > 0$.
Neka je $m_1 \in \mathcal{M}$ proizvoljna poruka. Tada je

$$P(C = c \,|\, M = m_1) = p_c \tag{2.18}$$

kao posledica (2.12) i (2.13). Dalje je

$$\begin{aligned} P(C = c) &= \sum_{m_1 \in \mathcal{M}} P(C = c \,|\, M = m_1) \cdot P(M = m_1) && (2.19)\\ &= \sum_{m_1 \in \mathcal{M}} p_c \cdot P(M = m_1) \\ &= p_c \cdot \sum_{m_1 \in \mathcal{M}} P(M = m_1) \\ &= p_c && (2.20)\\ &= P(E_K(m) = c) \\ &= P(E_K(M) = c \,|\, M = m) \\ &= P(C = c \,|\, M = m) \end{aligned}$$

Koristeći (2.14) i (2.20) dobijamo

$$P\left(M = m \,|\, C = c\right) = P\left(M = m\right)$$

što je i trebalo dokazati. ■

Prethodna definicija apsolutne sigurnosti zasniva se na zahtevu da su poruka i njen šifrat nezavisne slučajne promenljive, jednakost (2.11), što po teoriji informacija implicira da je količina informacija koju šifrat nosi o poruci koju predstavlja jednaka nuli. Intuitivno uslov da napadač nije u stanju da ekstrahuje informacije o poruci čiji šifrat poseduje može se opisati na sledeći način.

Neka su napadaču poznate dve poruke $m_0, m_1 \in \mathcal{M}$ i šifrat $c$ jedne od njih ali napadač ne zna koje. Ako napadač nije u stanju da odredi koja je poruka šifrovana sa verovatnoćom većom od jedne polovine tada sistem smatramo apsolutno sigurnim. Zahtevana verovatnoća mora biti veća od jedne polovine jer nasumični izbor će davati tačan rezultat sa verovatnoćom jedna polovina.

**Definicija 4** ***(Igra nerazlučivosti sa napadačem u apsolutno sigurnim sistemima)***
*Neka je dat šifarski sistem* $\Pi = (G, E, D)$ *i napadač* $\mathcal{A}$

1. *Napadaču* $\mathcal{A}$ *bira par poruka* $m_0, m_1$.
2. *U skladu sa odgovarajućim uniformnim raspodelama bira se bit* $b \in \{0, 1\}$ *i algoritmom* $G$ *generiše ključ* $k \in \mathcal{K}$ *Izračuna se*

   $$E_k\left(m_b\right) = c.$$

   *Vrednost* $c$ *se naziva test šifrat i prosleđuje se napadaču.*
3. $\mathcal{A}$ *sprovodi svoja računanja i saopštava dobijenu vrednost bita* $b'$.
4. *Rezultat igre je* 1 *ako je* $b = b'$, *inače je* 0.
   *Igra nerazlučivosti sa napadačem se označava sa* $PrivK^{eav}_{\mathcal{A},\Pi}$. *Ako je rezultat igre jednak* 1 *pišemo* $PrivK^{eav}_{\mathcal{A},\Pi} = 1$ *i kažemo da je napadač uspeo u napadu.*

**Teorema 5** *Šifarski sistem* $\Pi = (G, E, D)$ *je apsolutno siguran ako i samo ako je*

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi} = 1\right) = \frac{1}{2}.$$

**Dokaz.** Dokažimo prvo da ako je $\Pi = (G, E, D)$ apsolutno siguran sistem tada je $P\left(PrivK^{eav}_{\mathcal{A},\Pi} = 1\right) = \frac{1}{2}$.
Neka je $\mathcal{A}$ proizvoljan napadač i neka su njegove odabrane poruke $m_0, m_{1.}$ Koristeći Teoremu 3 za odabrane poruke $m_0, m_1 \in \mathcal{M}$ i svako $c \in \mathcal{C}$ važi

$$P\left(E_K\left(m_0\right) = c\right) = P\left(E_K\left(m_1\right) = c\right). \tag{2.21}$$

Uvedimo sledeće oznake

$$\begin{aligned} \mathcal{C}_0 &= \{c \,|\, c \in \mathcal{C} \,\wedge\, b' = 0\} \\ \mathcal{C}_1 &= \{c \,|\, c \in \mathcal{C} \,\wedge\, b' = 1\} \end{aligned} \tag{2.22}$$

i prema tome, jer je$\mathcal{A}$ deterministički algoritam, važi

$$\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1. \tag{2.23}$$

Primenom teoreme potpune verovatnoće, [59], imamo

$$\begin{aligned} &PP\left(PrivK^{eav}_{\mathcal{A},\Pi} = 1\right) \\ &=P\left(b' = 0 \,|\, b = 0\right) \cdot P\left(b = 0\right) + P\left(b' = 1 \,|\, b = 1\right) \cdot P\left(b = 1\right) \end{aligned} \tag{2.24}$$

Pošto se bit $b \in \{0, 1\}$ bira u skladu sa uniformnom raspodelom, koristeći (2.22) i (2.23) u (2.24) dobijamo

$$\begin{aligned} &P\left(PrivK^{eav}_{\mathcal{A},\Pi} = 1\right) = \\ &= \frac{1}{2} \cdot P\left(b' = 0 \,|\, b = 0\right) + \frac{1}{2} \cdot P\left(b' = 1 \,|\, b = 1\right) \\ &= \frac{1}{2} \cdot \sum_{c \in \mathcal{C}_0} P\left(E_K\left(m_0\right) = c\right) + \frac{1}{2} \cdot \sum_{c \in \mathcal{C}_1} P\left(E_K\left(m_1\right) = c\right) \end{aligned} \tag{2.25}$$

Koristeći (2.21) u (2.25) dalje sledi

$$\begin{aligned}
&P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)= \\
&=\frac{1}{2}\cdot\sum_{c\in\mathcal{C}_0}P\left(E_K\left(m_0\right)=c\right)+\frac{1}{2}\cdot\sum_{c\in\mathcal{C}_1}P\left(E_K\left(m_1\right)=c\right) \\
&=\frac{1}{2}\cdot\sum_{c\in\mathcal{C}_0}P\left(E_K\left(m_0\right)=c\right)+\frac{1}{2}\cdot\sum_{c\in\mathcal{C}_1}P\left(E_K\left(m_0\right)=c\right) \\
&=\frac{1}{2}\cdot\left(\sum_{c\in\mathcal{C}_0}P\left(E_K\left(m_0\right)=c\right)+\sum_{c\in\mathcal{C}_1}P\left(E_K\left(m_0\right)=c\right)\right) \\
&=\frac{1}{2}\cdot\sum_{c\in\mathcal{C}_0\cup\mathcal{C}_1}P\left(E_K\left(m_0\right)=c\right) \\
&=\frac{1}{2}\cdot\sum_{c\in\mathcal{C}}P\left(E_K\left(m_0\right)=c\right) \\
&=\frac{1}{2}
\end{aligned} \tag{2.26}$$

čime je dokaz gotov.

Dokažimo sada da ako je $P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)=\frac{1}{2}$ tada je sistem apsolutno siguran. Pretpostavimo suprotno, da je $P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)=\frac{1}{2}$ i da sistem nije apsolutno siguran.

Tada po Teoremi 3 postoje poruke $m_0, m_1 \in \mathcal{M}$ i šifrat $c_0 \in C$ tako da je

$$P\left(E_K\left(m_0\right)=c_0\right)\neq P\left(E_K\left(m_1\right)=c_0\right) \tag{2.27}$$

U igri razlučivanja $\mathcal{A}$ kao svoje poruke bira $m_0, m_1$. Ako test šifrat označimo sa $c$ tada $\mathcal{A}$ svoj bit $b'$ određuje na sledeći način

$$b'=\begin{cases} 0 & c=c_0 \\ \\ U_{\{0,1\}} & c\neq c_0 \end{cases} \tag{2.28}$$

gde $U_{\{0,1\}}$ označava slučajan izbor jedne od dve vrednosti u skladu sa uniformnom raspodelom.

Koristeći formulu potpune verovatnoće, slično kao u (2.24) dobijamo

$$\begin{aligned}
&P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)= \\
&=\frac{1}{2}\cdot P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,M=m_0\right)+\frac{1}{2}\cdot P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,M=m_1\right).
\end{aligned} \tag{2.29}$$

Posmatrajmo sada $P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,M=m_0\right)$. Da bi napadač bio uspešan pod uslovom da je odabrana i šifrovana poruka $m_0$ tada test šifrat mora biti jednak $c_0$ ili ako to nije slučaj onda odabrani bit mora bit 0. Dakle

$$\begin{aligned}
&P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,M=m_0\right)=\\
&\quad=P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\wedge E_K\left(m_0\right)=c_0\right)+P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\wedge E_K\left(m_0\right)\neq c_0\right)\\
&\quad=P\left(E_K\left(m_0\right)=c_0\right)+P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\wedge E_K\left(m_0\right)\neq c_0\right) \qquad (2.30)\\
&\quad=P\left(E_K\left(m_0\right)=c_0\right)+P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,E_K\left(m_0\right)\neq c_0\right)\cdot P\left(E_K\left(m_0\right)\neq c_0\right)\\
&\quad=P\left(E_K\left(m_0\right)=c_0\right)+\frac{1}{2}\cdot P\left(E_K\left(m_0\right)\neq c_0\right)
\end{aligned}$$

Na potpuno isti način vodeći računa o tome da je $P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\wedge E_K\left(m_1\right)=c_0\right)=0$ zbog (2.28) dobijamo

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\,|\,M=m_1\right)=\frac{1}{2}\cdot P\left(E_K\left(m_1\right)\neq c_0\right). \qquad (2.31)$$

Zamenjujući rezultate (2.30) i (2.31) u (2.29) dobijamo

$$\begin{aligned}
&P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)=\\
&\quad=\frac{1}{2}\cdot\left(P\left(E_K\left(m_0\right)=c_0\right)+\frac{1}{2}\cdot P\left(E_K\left(m_0\right)\neq c_0\right)\right)\\
&\quad+\frac{1}{2}\cdot\frac{1}{2}\cdot P\left(E_K\left(m_1\right)\neq c_0\right)\\
&\quad=\frac{1}{2}\cdot\left(P\left(E_K\left(m_0\right)=c_0\right)+\frac{1}{2}\cdot\left(1-P\left(E_K\left(m_0\right)=c_0\right)\right)\right)\\
&\quad+\frac{1}{2}\cdot\frac{1}{2}\cdot P\left(E_K\left(m_1\right)\neq c_0\right) \qquad (2.32)\\
&\quad=\frac{1}{4}\cdot\left(1+P\left(E_K\left(m_0\right)=c_0\right)+P\left(E_K\left(m_1\right)\neq c_0\right)\right)
\end{aligned}$$

Sada imamo

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)=\frac{1}{4}\cdot\left(1+P\left(E_K\left(m_0\right)=c_0\right)+P\left(E_K\left(m_1\right)\neq c_0\right)\right) \qquad (2.33)$$

i koristeći (2.27) dobijamo

$$\begin{aligned}
&\frac{1}{4}\cdot\left(1+P\left(E_K\left(m_0\right)=c_0\right)+P\left(E_K\left(m_1\right)\neq c_0\right)\right)\neq \qquad (2.34)\\
&\neq\frac{1}{4}\cdot\left(1+P\left(E_K\left(m_1\right)=c_0\right)+P\left(E_K\left(m_1\right)\neq c_0\right)\right)=\frac{1}{2}
\end{aligned}$$

Sada iz (2.33) i (2.34) dobijamo

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi}=1\right)\neq\frac{1}{2}$$

što je u suprotnosti sa polaznom pretpostavkom pa je tvrđenje dokazano. ■

Apsolutno sigurni šifarski sistemi cenu svoje snage plaćaju i nekim ograničenjima. Prvo i osnovno ograničenje odnosi se na veličine prostora ključeva i prostora poruka.

**Teorema 6** *Ako je šifarski sistem* $(G, E, D)$ *apsolutno siguran sa prostorom poruka* $\mathcal{M}$ *i prostorom ključeva* $\mathcal{K}$ *tada je* $|\mathcal{K}| \geq |\mathcal{M}|$.

**Dokaz.** Pretpostavimo suprotno, da je sistem apsolutno siguran i da je $|\mathcal{K}| < |\mathcal{M}|$. Neka slučajna promenljiva $M$ ima uniformnu raspodelu i neka je $c \in C$ takvo da je $P(c) > 0$. Označimo sa $\mathcal{M}(c)$ skup svih poruka $m \in \mathcal{M}$ takvih da postoji $c \in C$ i da je $D_K(c) = m$, formalno

$$\mathcal{M}(c) = \{m \,|\, m \in \mathcal{M} \wedge (\exists k \in \mathcal{K})(D_k(c) = m)\}. \tag{2.35}$$

Jasno je da je $|\mathcal{K}| \geq |\mathcal{M}(c)|$ jer u suprotnom proces dešifrovanja ne bi bio jednoznačan. Na osnovu $|\mathcal{K}| \geq |\mathcal{M}(c)|$ i pretpostavke da je $|\mathcal{K}| < |\mathcal{M}|$ dobijamo da je

$$|\mathcal{M}(c)| < |\mathcal{M}| \tag{2.36}$$

a ovo znači da

$$(\exists m_1)(m_1 \in \mathcal{M} \wedge m_1 \notin \mathcal{M}(c)). \tag{2.37}$$

Međutim zbog (2.37) imamo

$$P(M = m_1 \,|\, C = c) = 0$$

odnosno

$$P(M = m_1 \,|\, C = c) \neq P(M = m_1)$$

što je kontradikcija sa pretpostavkom da je sistem apsolutno siguran pa pretpostavka $|\mathcal{K}| < |\mathcal{M}|$ ne može biti tačna te imamo $|\mathcal{K}| \geq |\mathcal{M}|$ što je i trebalo dokazati. ■

Lako se vidi da je za jednoznačno dešifrovanje neophodno $|\mathcal{C}| \geq |\mathcal{M}|$.

#### 2.4.1.1 "One Time Pad" sistem

Vernam je 1919 patentira šifarski sistem, [60], koji je danas poznat pod imenom "One Time Pad" ali u to vreme nije postojao aparat kojim bi se verifikovala snaga

tog sistema. Šenon je dvadesetak godina kasnije u svom radu [11] definisao kriterijum apsolutne sigurnosti za šifarske sisteme i dokazao da je Vernamov sistem apsolutno siguran te se taj sistem otuda vezuje za Šenonovo ime.

Definišimo sada "One Time Pad" sistem.

**Definicija 7** *Neka je dat prirodan broj $l > 0$, i neka za prostor poruka $\mathcal{M}$ prostor šifrata $\mathcal{C}$ i prostor ključeva $\mathcal{K}$ važi $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^l$. Šifarski sistem $(G, E, D)$ ćemo zvati "One Time Pad" i označavati sa OTP ako*

- *Algoritam generatora ključeva $G$ produkuje ključeve po uniformnoj raspodeli, $P(K = k) = \frac{1}{2^l}$.*
- *Algoritam šifrovanja $E$ za dati ključ $k \in \{0,1\}^l$ i poruku $m \in \{0,1\}^l$ formira šifrat $c$ sa*
$$c = k \oplus m.$$
- *Algoritam dešifrovanja $D$ za dati ključ $k \in \{0,1\}^l$ i šifrat $c \in \{0,1\}^l$ formira poruku $m$ sa*
$$m = k \oplus c.$$

Dokažimo sada da je OTP apsolutno siguran šifarski sistem.

**Teorema 8** *Šifarski sistem OTP je apsolutno siguran.*

**Dokaz.** Neka su proizvoljno $c \in C$ i $m \in \mathcal{M}$ takvi da je $P(M = m) > 0$. Tada iz definicije za OTP sledi

$$\begin{aligned} P(C = c \,|\, M = m) &= P(K \oplus m = c \,|\, M = m) \\ &= P(K = c \oplus m \,|\, M = m) \end{aligned} \tag{2.38}$$

Sada, koristeći činjenicu da se ključevi generišu u skladu sa uniformnom raspodelom i nezavisno od $M$ dobijamo

$$P(K = c \oplus m \,|\, M = m) = P(K = c \oplus m) = \frac{1}{2^l} \tag{2.39}$$

Koristeći (2.38) i (2.39) dobijamo

$$P(C = c \,|\, M = m) = \frac{1}{2^l} \tag{2.40}$$

Neka slučajna promenljiva $M$ ima proizvoljnu funkciju raspodele i neka je $c \in C$ proizvoljno. Tada

$$\begin{aligned} P(C=c) &= \sum_{m\in\mathcal{M}} P(C=c \mid M=m)\cdot P(M=m) \qquad (2.41)\\ &= \frac{1}{2^l}\sum_{m\in\mathcal{M}} P(M=m) \qquad \text{koristeći jednačinu (2.40)}\\ &= \frac{1}{2^l} \end{aligned}$$

Koristeći Bajesovu teoremu, [59], odnosno jednačinu (2.14) dobijamo

$$P(M=m \mid C=c) = \frac{P(C=c \mid M=m)\cdot P(M=m)}{P(C=c)} \qquad (2.42)$$

Zamenjujući rezultate (2.40) (2.41) u (2.42) dobijamo

$$\begin{aligned} P(M=m \mid C=c) &= \frac{\frac{1}{2^l}\cdot P(M=m)}{\frac{1}{2^l}}\\ &= P(M=m) \end{aligned}$$

što u skladu sa definicijom 2 znači da je OTP apsolutno siguran sistem. ■

### 2.4.2 Praktično sigurni šifarski sistemi

U prethodnom delu pored kvaliteta apsolutno sigurnih šifrskih sistema konstatovana su i neka njima inherentna ograničenja. To je bio razlog uvođenja novog koncepta, praktične sigurnosti (computational secrecy) kao načina za pravevilaženje pomenutih ograničenja. Teorijska razrada ovog koncepta kao dodatni rezultat donela je i formalnu definiciju pseudoslučajnosti odnosno pseudoslučajnih generatora.

Apsolutno sigurni šifraski sistemi postižu savršenu zaštitu tako što ne dozvoljavaju da se bilo koja količina informacija o zaštićenoj poruci prenese u šifrat. Posledica toga je da čak ni kada napadač poseduje neograničene računarske resurse i procesnu snagu iz šifrata ne može da zaključi ništa o sadržaju poruke koju šifrat predstavlja. U mnogim svakodnevnim životnim situacija zaštita tog nivoa nije neophodna jer je potreba za tajnošću zaštićenog sadržaja vremenski ograničena. Ideja koja se prirodno javila i vodila u tom smeru je da se dozvoli prelivanje izvesne količine informacija u šifrat ali da ta količina informacija bude dovoljno mala da napadač sa svojim resursima ne bude u stanju da je produktivno iskoristi.

Dakle dve relaksacije u odnosu na apsolutno sigurne šifarske sisteme, informaciono teoretski model, su:

1. Bezbednost se u ovom modeli razmatra u odnosu na efikasnog napadača, u smislu teorije složenosti računanja, koji za napad ima neko konačno ali ograničeno i dostupno vreme, na primer deset, dvadeset sto ... godina. Ako je sistem tako dizajniran da neophodne resurse za izvođenje napada nije moguće obezbediti sistem se smatra sigurnim.

2. Ako u slučaju dostupnog vremena i realno mogućih resursa napadač može da ostvari svoje ciljeve tada verovatnoća njegovog uspeha mora biti zanemarljivo mala.

Načini za formalizaciju ovih ideja prikazuju se u sledećim odeljcima ovog dela.

### 2.4.3 Model procene sigurnosti zasnovan na teoriji složenosti računanja

Ovaj metod procene sigurnosti kriptografskih algoritama svoje korene ima u teoriji složenosti računanja. U ovom modelu uvodi se sigurnosni parametar $n \in \mathbb{N}$ koji se može posmatrati kao dužina kriptografskog ključa datog kriptografskog algoritma. Neformalno govoreći, ovde se kriptografski algoritam smatra bezbednim za upotrebu ako je verovatnoća uspeha efikasnog napada mala.

Pod efikasnim napadačem, odnosno napadom, smatra se svaki napadač koji je u stanju da izvodi probabilističke algoritme čije se trajanje u vremenu opsuje polinomijalnom funkcijom $p(t)$. Radi jednostavnosti, probabilističke algoritme čije je izvršavanje polinomijalno po vremenu, nadalje će se označavati sa $PPT$. U formalnom modeliranju snage napadača izabrani su probabilistički polinomijalni algoritmi iz dva razloga. Prvo klasa probabilističkih polinomijalnih algoritama je šira od klase determinističkih polinomijalnih algoritama odakle sledi da napadač raspolaže većom snagom. Drugo, strane koje učestvuju u komunikaciji raspolažu probabilističkim mogućnostima, izbor ključeva i drugo, pa je realno pretpostavati da takvu mogućnost ima i napadaču.

Da bi se prethodni neformalni opis formalizovao moramo formalizovati pojam "mala verovatnoća".

**Definicija 9** *Za funkciju* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *kažemo da je beznačajna ako za svaki polinom* $p$ *postoji prirodan broj* $n_0$ *takav da kada je* $n > n_0$ *tada je* $p(n) > 0$ *i* $f < \frac{1}{p(n)}$.

Za neki događaj $A(n)$ koji zavisi od $n$ kažemo da ima beznačajnu verovatnoću ako je $P(A(n)) < f$ kada je $n > n_0$ gde je $f$ beznačajna funkcija. U praksi se češće koristi izraz $P(A(n)) < \frac{1}{p(n)}$, što je ekvivalentno.

Prethodno data definicija kriptografskog sistema se mora modifikovati jer sada kao element sistema figuriše i sigurnosni parametar $n$ -dužina ključa.

**Definicija 10** *Simetričan kriptografski sistem sastoji se od tri PPT algoritma* $(G, E, D)$ *tako da*

1. *Algoritam* $G$ *za ulazni parametar* $n$ *generiše ključ* $k$ *tako da je* $|k| \geq n$.
2. *Algoritam* $E$ *za ulazne parametre* $k$ *i* $m \in \{0,1\}^*$*kao izlaz daje šifrat* $c$, $E_k(m) = c$.
3. *Algoritam dešifrovanja* $D$ *koji za dati ključ* $k$ *i neki šifrat* $c$ *kao rezultat daje* $m \in \{0,1\}^*$, *ako takva poruka postoji ili simbol* $\perp$ *kao indikator greške ako takva poruka ne postoji.*
4. *Neophodno je da za svaki ključ* $k$, *i svaku poruku* $m \in \{0,1\}^*$ *važi* $D_k(E_k(m)) = m$.

Kao što je ranije rečeno da bi se formalizovao pojam sigurnosti kriptografskog algoritma i ocenila njegova snaga mora se formalno odrediti pojam napada na kriptografski algoritam. Napad na kriptografski algoritam se identifikuje kroz dve komponente. Prva je sposobnost napadača koja se odslikava u njegovoj računarskoj snazi i informacijama i podacima koje u vezi sa kriptografskim algoritmom poseduje a druga je cilj koji napadom želi da postigne.

U tom smislu, računarske sposobnosti napadača ćemo opisati kao polinomijalno probabilističke po dužini vremena napada, a znanje o sistemu na posedovanje jednog šifrata. Ove pretpostavke o sposobnosti napadača ni u kom slučaju ne prejudiciraju njegovu strategiju i algoritme napada. Ovo je suštinska karakteristika buduće definicije sigurnosti kriptografskih algoritama jer se tako opisuje sigurnost kriptografskog algoritma u odnosu na svakog polinomijalno ograničenog napadača bez obzira na algoritme koje primenjuje.

Formalno određivanje druge komponente, napadačevog cilja, je delikatan zadatak. Intuitivno ideja se sastoji u tome da napadač nije u stanju da sazna informacije o otvorenom tekstu koje bi mogao efektivno da koristi. U definiciji apsolutno sigurnih kriptografskih algoritama količina informacija koje napadač može da sazna je nula. U ovom slučaju dozvoljava se da se neka, beznačajna, količina informacija odlije ka napadaču ali mu ta količina informacija nije dovoljna da bi mogao da zaključi bilo šta o poruci čiji mu je šifrat dostupan. Ideja se sastoji u eksperimentu koji ćemo zvati igra razlučivanja. Igra se odvija na sledeći način.

Odaberu se dve poruke $m_0, m_1 \in \mathcal{M}$, ključ $k \in \mathcal{K}$ i bit $b \in \{0,1\}$ u skladu sa odgovarajućim uniformnim raspodelama. Izračuna se $E_k(m_b) = c$. Sada se napadaču prosledi $\{m_0, m_1, c\}$. Njegov zadatak je da odredi koju poruku predstavlja šifrat. Formalna definicija je sledeća.

**Definicija 11** ***(Igra nerazlučivosti sa napadačem u praktično sigurnim sistemima)***
*Neka je dat šifarski sistem* $\Pi = (G, E, D)$, *bezbednosni parametar* $n$ *i napadač* $\mathcal{A}$

1. *Napadaču* $\mathcal{A}$ *je poznata vrednost bezbednosnog parametra* $n$ *i par poruka* $m_0, m_1$ *za koje važi* $|m_0| = |m_1|$.

2. *U skladu sa odgovarajućim uniformnim raspodelama bira se bit* $b \in \{0,1\}$ *i algoritmom* $G$ *generiše ključ* $k \in \mathcal{K}$ *Izračuna se*

$$E_k(m_b) = c.$$

   *Vrednost* $c$ *se naziva test šifrat i prosleđuje se napadaču.*

3. $\mathcal{A}$ *sprovodi svoja računanja i saopštava dobijenu vrednost bita* $b'$.

4. *Rezultat eksperimenta je* 1 *ako je* $b = b'$, *inače je* 0.
   *Igra nerazlučivosti sa napadačem se označava sa* $PrivK^{eav}_{\mathcal{A},\Pi}(n)$. *Ako je rezultat igre jednak* 1 *pišemo* $PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1$ *i kažemo da je napadač uspeo u napadu.*

Posmatrajući prethodnu definiciju jasno je da napadač uvek može uspeti sa verovatnoćom jedna polovina generišući bit $b'$ uniformno ali ta strategija mu ne daje nikakve informacije o $m$. Da bi bio u stanju da ekstrahuje informacije o šifrovanoj poruci ta verovatnoća mora biti značajno veća od jedne polovine. Imajući ovo

u vidu prirodno je kriptografski algoritam u ovako definisanoj igri nerazlučivosti smatrati sigurnim ako je verovatnoća uspeha napadača beznačajno veća od jedne polovine. To nas upućuje na sledeću definiciju.

**Definicija 12** ***(EAV-siguran sistem)***
*Za simetričan kriptografski sistem* $\Pi = (G, E, D)$ *i bezbednosni parametar* $n$ *kažemo da sistem* $\Pi$ *ima nerazlučive šifrate u prisustvu napadača odnosno da je EAV-siguran ako za sve probabilističke polinomijalne po vremenu napadače* $\mathcal{A}$ *postoji beznačajna funkcija* $negl$ *tako da za sve* $n$ *važi*

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + negl(n) \tag{2.43}$$

*Navedena verovatnoća se računa u odnosu na funkcije raspodele slučajnih promenljivih koje se koriste u igri.*

Termin $EAV$-siguran je ovde upotrebljen zbog rasprostranjenosti u anglosaksonskoj literaturi ($EAV$-secure od engleske reči *"eavsdropper"* kojom se označava napadač).

Sada kada imamo definicije dva tipa sigurnosti kriptografskih algoritama prirodno je upitati kakav je odnos vlada među njima. Taj odnos se manifestuje na dva načina.

Prvo, što se tiče nivoa sigurnosti apsolutno sigurni kriptografski algoritmi poseduju viši nivo bezbednosti od praktično sigurnih kriptografskih algoritama. To se zaključuje na sledeći način.

Po teoremi 5 sistem je apsolutno siguran ako i samo ako je

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi} = 1\right) = \frac{1}{2} \tag{2.44}$$

a po definiciji 12 sistem $\Pi$ je praktično siguran ako i samo ako je

$$P\left(PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + negl(n). \tag{2.45}$$

Upoređujući (2.44) i (2.45) sledi da je svaki apsolutno siguran sistem u isto vreme i praktično siguran sistem.

Drugo, po teoremi 6 imamo da je $|\mathcal{K}| \geq |\mathcal{M}|$ odnosno $H(\mathcal{K}) \geq H(\mathcal{M})$, [11], što implicitno znači da u nekom optimalnom kodiranju ključeva i poruka u apsolutno sigurnom šifarskom sistemu ključ mora biti najmanje iste dužine kao i poruka. Kod praktično sigurnih kriptografskih algoritama moguće su konstrukcije, pseudoslučajni generatori, koje na osnovu sigurnosnog parametra $n$ i inicijalne vrednost

*seed* koristeći algoritam $G$ generišu ključ za šifrovanje. Na taj način se ublažava problem generisanja i distribucije ključeva koji je inherentan apsolutno sigurnim šifarskim sistemima.

Koristeći ovaj pristup za simetričan šifarski sistem $\Pi$ mogu se dokazati sledeće činjenice:

- Sistem $\Pi$ je $EAV-$siguran ako se verovatnoće uspeha napadača kada se odabere poruka $m_0$ i kada se odabere poruka $m_1$ beznačajno razlikuju,

$$\left|P\left(PrivK^{eav}_{\mathcal{A},\Pi}\left(n,m_0\right)=1\right)-P\left(PrivK^{eav}_{\mathcal{A},\Pi}\left(n,m_1\right)=1\right)\right|\leq negl\left(n\right).$$

- Za proizvoljnog $PPT$ napadača $\mathcal{A}$ verovatnoća otkrivanja $i-$tog bita poruke na osnovu njenog šifrata je beznačajno veća od jedne polovine

$$P\left(\mathcal{A}\left(n,E_k\left(m\right)=m^i\right)\right)\leq\frac{1}{2}+negl\left(n\right).$$

- Za proizvoljne $PPT$ napadače $\mathcal{A}$, $\mathcal{A}'$ i proizvoljnu funkciju $f$ verovatnoća da napadač $\mathcal{A}$ znajući $n$ i $E_k\left(m\right)$ otkrije $f\left(m\right)$ se beznačajno razlikuje od verovatnoće da napadač $\mathcal{A}'$ znajući $n$ otkrije $f\left(m\right)$

$$\left|P\left(\mathcal{A}\left(n,E_k\left(m\right)\right)=f\left(m\right)\right)-P\left(\mathcal{A}'\left(n\right)=f\left(m\right)\right)\right|\leq negl\left(n\right).$$

- Moguće je formalno definisati pseudoslučajne generatore.

Dokazi prethodnih činjenica i više o ovom pristupu kao i obiman broj referenci može se naći u [12].

### 2.4.4 Model procene sigurnosti zasnovan na teoriji složenosti izvršavanja algoritama

Ovaj pristup predstavlja jedan praktičniji i manje formalan pristup problemu bezbednosti kriptografskih algoritama ali ipak sa logički i formalno utemeljenim zaključcima o pokazateljima njegove snage. Kriptografski sistem se označava sa $\Pi=(G,E,D)$ gde su $G,E,D$ funkcije ekspanzije ključa, šifrovanja i dešifrovanja redom sa prethodno definisanim značenjima. Napadačevu računsku snagu ćemo svrstavamo u $PPT$ klasu a njegovi potencijalni ciljevi i dostupne informacije određuju se u daljem tekstu.

Teorija složenosti izvršavanja algoritama se bavi procenom složenosti izvršavanja algoritma prilikom rešavanja različitih problema u smislu identifikacije i kvantifikovanja neophodnih resursa da bi se postavljeni zadatak rešio. Najčešće razmatrani resursi su vreme izvršavanja, angažovana električna energije i količina neophodne memorije. Ovaj pristup pretpostavlja da napad na predmetni kriptografski sistem $\Pi$ bude takav da se može raščlaniti na zadatke za koje su poznati algoritmi koji ih rešavaju, da se primene oni algoritmi koji su najefikasniji, u smislu angažovanih resursa, i da se njihovom superpozicijom realizuje napad i dobije ocena ukupne složenosti napada. Ako je najbolji poznati napad na dati kriptografski sistem $\Pi$ takav da nije moguće koncentrisati resurse koje takav napad zahteva (vreme izvršavanja, količina neophodne električne energije i memorijski kapacitet) tada se takav kriptografski sistem $\Pi$ smatra praktično sigurnim, odnosno sigurnim sa stanovišta složenosti izvršavanja algoritama. Ovaj pristup se često primenjuje u praksi i na taj način je na primer procenjivana kriptografska snaga kriptografskog algoritma AES, [62].

Za napade koji pripadaju ovoj klasi postoji nekoliko karakterističnih pristupa:

- Tehnika ekvivalentnih transformacija – napadač pokušava da nađe drugačije predstavljanje kriptografskog sistema $\Pi$, sa ekvivalentnom funkcionalnošću, koje omogućava lakšu analizu i efikasnije napade;
- Strukturna analiza – napadač sprovodi strukturnu analizu definisanog kriptografskog sistema $\Pi$ i razlaže ga na nezavisne funkcionalne blokove za koje je lakše sprovesti kriptoanalizu. Ova tehnika je poznata pod imenom "Divide and Conquere";
- Statistička analiza – napadač sprovodi iscrpnu teorijsku i eksperimentalnu statističku analizu sa ciljem da uoči statističke anomalije kriptografskog sistema $\Pi$. Ako postoje, anomalije se mogu iskoristiti za pokušaje dešifrovanja zaštićenih poruka, za uspostavljanje veza između elemenata kriptografskog sistema $\Pi$ i elemenata primenjenog ključa ili za neke druge pogodne tehnike kriptoanalize.

Karakteristike kriptografskog sistema $\Pi$ koje utiču na mogućnost sprovođenja određenih vrsta napada su:

1. Veličina perioda generisanih nizova u kriptografskom sistemu $\Pi$;

2. Veličina linearne složenosti generisanih nizova u kriptografskom sistemu $\Pi$, profila linearne složenosti generisanih nizova u kriptografskom sistemu $\Pi$, k-linearne složenosti generisanih nizova u kriptografskom sistemu $\Pi$;

3. Veličina algebarskog stepena funkcionalnih blokova, veličina stepena nelinearnosti funkcionalnih blokova i veličina korelacione imunosti;

4. Konfuzija: svaki bit šifrata mora biti kompleksna i neprediktabilna transformacija svih ili najvećeg dela bita ključa;

5. Difuzija: svaki bit ključa mora da utiče na što veći broj bita generisanog šifrata;

6. Statističke osobine šifrata i generisanih nizova u procesu šifrovanja;

7. Ponašanje u odnosu na lavinski efekat i striktni lavinski efekat. Lavinski efekat se odnosi na ponašanje kriptografskog algoritma kada se isti otvoreni tekst šifruje ključevima koji se razlikuju u malom broju bita. Poželjno je da se u tom slučaju šifrati razlikuju u što većem broju bita. Kod striktnog lavinskog efekta zahtev je da se ključevi razlikuju u jednom bitu a šifrati u polovini bita. Ova karakteristika se odnosi na svaki bit ključa.

Ovaj model kriptografske bezbednosti se razlikuje od prethodnih po tome što pored sposobnosti pretpostavlja i strategiju napadača ograničavajući ga na javno poznate relevantne karakteristike i napade na kriptografske algoritme. Ako su pretpostavke o težini relevantnih problema ispravne i najbolji poznati algoritmi za njihovo rešavanje zbilja optimalni tada su i zaključci o snazi algoritma formalno zasnovani. Neizvesnost verodostojnosti prihvaćenih pretpostavki, u slučaju primene ovog modela, zahteva kontinuiranu pažnju u pogledu izvedenih bezbednosnih zaključaka.

## 2.5 Bezbednosni modeli kriptografskih algoritama u praksi

Izloženi bezbednosni metodološki modeli za procenu snage kriptografskih algoritma su raznovrsni i po aparaturi koju koriste i po primenljivosti u stvarnom svetu.

Svest o potrebi formalizacije intuitivne ideje bezbednosti kriptografskih algoritma dovela je do značajnog iskoraka u teorijskom zasnivanju tog pojma. Formalno određenje kriptografskog algoritma kroz funkcije ekspanzije ključa, šifrovanja i dešifrovanja te prepoznavanje napadača kroz njegove sposobnosti i ciljeve uvelo je kriptografsku bezbednost u svet formalnih teorija i dokazivih zaključaka. Primenjuju se aparature različitih teorija sa različitim stepenima uspešnosti.

Teorija informacija je uspela da u potpunosti odredi apsolutno sigurne sisteme i da se verifikuje izvedene zaključke i karakterizacije u praksi. To je postignutom uglavnom, zbog vrlo preciznog i verodostojnog određenja napadača i njegovih sposobnosti. Napadač ima beskonačnu računarsku snagu i od informacija poseduje samo šifrat. Ugrožavanje ovih odrednica čini sistem nepouzdanim, [50], [51], [16].

Teorija složenosti izračunavanja je svoj model bezbednosti kriptografskih algoritama možda najkompletnije formalizovala i zaokružila. Složenost ovog modela leži u sledećim činjenicama:

- Svako novo određenje napadačevih sposobnosti promenom njegovih podataka informacija o sistemu šifrovanja zahteva novo određenje tipa napadača i novu definiciju bezbednosti kriptografskog algoritma za taj kontekst.
- Svaka promena napadačevog cilja zahteva novo određenje tipa napadača i novu definiciju bezbednosti kriptografskog algoritma za taj kontekst.
- Svaka nova realnost u mogućnostima napada zahteva novo određenje tipa napadača i novu definiciju bezbednosti kriptografskog algoritma za taj kontekst.
- Postoje teškoće u formalnom opisu realnih situacija u kojima se napadi mogu eventualno uspešno odigrati.

Ove činjenice usložnjavaju svet mogućih napada i njihovo formalno opisivanje a samim tim otežavaju izvođenje dokaza koji će se verodostojno odnositi na realan svet. Stoga se čine napori da se ta raznolikost u napadačkom svetu smanji tako što će se formalizovati generički tipovi znanja napadača, kao na strani 2, i njegovi ciljevi kao u definiciji 38.

Teorija složenosti izvršavanja kriptografskih algoritama premise bezbednosti kriptografskih algoritama nalazi u pretpostavkama o nepoznavanju polinomijalnih algoritama za rešavanje određenih vrsta problema. Pretpostavke su iskustvene i

stoga zasnovane na poverenju a ne na čvrstim dokazima. Ako se te pretpostavke shvate kao aksiome, preostali deo procesa konstrukcije dokaza kriptografske bezbednosti ovom metodom je potpuno formalno određen i pouzdan. Iako ova tehnika počiva na heurističkim osnovama njeni rezultati su se u praksi pokazali verodostojnim i dugotrajnim, [62].

Savremena kriptografija razvija aparaturu zasnivanja kriptografske bezbednosti na matematičkim metodama i formalnim dokazima. Takav pristup je u značajnoj meri unapredio kriptografske konstrukcije ali sve te tehnike i činjenice treba prihvatati na razuman način. Ne treba precenjivati snagu izvedenih dokaza. Dokaz se izvodi u odnosu na formalan opis sistema i napadača. Ako opis sistema nije verodostojan ili opis napadača nije primeren realnoj upotrebi kriptografskog algoritma tada ni dokaz ne donosi relevantnu informaciju u odnosu na realan svet. Drugačije rečeno dokaziva sigurnost u odnosu na neki kriptografski sistem ne znači nužno i njegovu sigurnost u realnom svetu.

## 2.6 Metodologija bezbednosne evaluacije kriptografskih algoritama

Metodologija bezbednosne evaluacije kriptografskog algoritma se bavi bezbednosnim karakteristikama kriptografskog algoritma kao takvog i ne bavi se bezbednosnim posledicama implementacije kriptografskog algoritma. Cilj metodologije bezbednosne evaluacije kriptografskih algoritama je definisanje sistematičnog skupa procedura i postupaka čiji rezultati ukazuju na stepen zaštite koji predmetni kriptografski algoritam omogućava

### 2.6.1 Kriptografski algoritmi bazirani na generatorima pseudoslučajnih brojeva i napadi na njih

Imajući u vidu da je svaki generator pseudoslučajnih brojeva konačan automat sa periodičnim izlazom jasno je da takv kriptografski sistem ne ispunjava Šenonove uslove i ne poseduje karakteristiku apsolutne bezbednosti. Zbog toga se moramo ograničiti na klasu praktično sigurnih algoritama za šifrovanje i procene sprovoditi u tom smeru primerenom metodologijom. Za takav pristup se pre svega moraju definisati pretpostavljeni ciljevi i mogućnosti napadača. U današnjoj teoriji, prema [63], [64], ciljevi potencijalnog napadača se mogu okarakterisati na sledeći način:

1. **Potpuni uspeh** – kada je napadač u stanju da otkrije sadržaj zaštićene poruke ili primenjeni tajni ključ;

2. **Funkcionalni uspeh (global deduction)** – kada je napadač u stanju da konstruiše funkcionalno ekvivalentne algoritme za šifrovanje i dešifrovanje ali mu to ne omogućava da dođe do ključa;

3. **Konstruktivni uspeh (instance of local deduction)** – kada je napadač u stanju da konstruiše prethodno nepoznate validne šifrate i njima odgovarajuće poruke;

4. **Konstrukcija raspoznavača (distinguishing algorithm)** – kada je napadač u stanju efektivno da razlikuje šifrat datim sistemom sa slučajno odabranim ključem od slučajnog niza.

Redosled ciljeva je dat po opadajućoj snazi tako da realizacija cilja $n$ povlači mogućnost realizacije cilja $n+1$ i nemogućnost realizacije cilja $n$ povlači nemogućnost realizacije cilja $n-1$. Na izbor cilja takođe utiču i napadaču dostupni podaci navedeni na strani 2.

Za potrebe ovog dokumenta uslove za bezbednost predmetnog kriptografskog algoritma se dodatno pooštravaju dajući napadaču veće mogućnosti nego što je uobičajeno prema gore navedenim ciljevima i dostupnim podacima.

Smatraćemo:

- Napadaču su, u skladu sa Kerhofsovim principom, [56], [57], poznati i struktura i parametri kriptografskog algoritma osim primenjenog ključa;

- Napadaču je poznat izlaz iz generatora pseudoslučajnog niza;

- Cilj napadača je da rekonstruiše šifrovanu poruku, primenjeni ključ ili da smanji entropiju primenjenog ključa.

Kao što smo videli, nije moguće dizajnirati generator pseudoslučajnih brojeva i na njemu baziran sistem za šifrovanje koji bi imao bezbednosni nivo apsolutne sigurnosti, teorema 6. Sledeći poželjan cilj dizajnera kriptografskog algoritma je da u procesu sinteze kriptografskog algoritma definiše takav kriptografski algoritam za koji će biti u stanju da dokaže bezbednost primenom aparature teorije složenosti izračunavanja. Na žalost, u praksi, ovo vrlo često nije moguće i moramo se okrenuti mogućnostima koje nam pruža aparatura teorije složenosti izvršavanja

algoritama. U tom kontekstu dovoljno je pokazati da praktično nije moguće smanjiti entropiju primenjenog tajnog ključa na osnovu poznavanja izlaznog niza iz generator pseudoslučajnih brojeva. Ovo implicitno znači da napadač nema drugih mogućnosti za otkrivanje primenjenog ključa osim postupka potpune pretrage po prostoru svih mogućih ključeva.

Tipovi napada koje napadač može pokušati radi ostvarenja prethodno navedenog cilja, a koji proizilaze iz prethodno razmatranih teorijskih pristupa pri utvrđivanju stepena sigurnosti kriptografskog algoritma, su sledeći:

**A1.** Pokušaj rekonstrukcije ključa ili nekih njegovih delova direktnim ili indirektnim postupkom potpune pretrage po skupu svih mogućih ključeva.

**A2.** Pokušaj rekonstrukcije ključa ili nekih njegovih delova rešavanjem sistema algebarskih jednačina pridruženog generatoru niza pseudoslučajnih brojeva.

**A3.** Pokušaj rekonstrukcije otvorenog teksta korišćenjem svojstva generatora pseudoslučajnih brojeva u slučaju lošeg ponašanja u odnosu na avalanš efekat ili strogi avalanš efekat

**A4.** Mogućnost napada metodom Kerhofsa.

**A5.** Pokušaj rekonstrukcije ključa ili nekih njegovih delova ekvivalentnom zamenom generatora pseudoslučajnih brojeva ili nekog njegovog dela konačnim automatom koji je pogodan za kriptoanalizu.

**A6.** Pokušaj rekonstrukcije ključa ili nekih njegovih delova podelom generatora pseudoslučajnih brojeva na funkcionalne delove koji se mogu nezavisno analizirati.

**A7.** Statističko dešifrovanje, tj. pokušaj rekonstrukcije ključa, otvorenog teksta ili njihovih delova korišćenjem odstupanja generisanog niza pseudoslučajnih brojeva ili nekih nizova unutar generatora pseudoslučajnih brojeva od idealnog slučajnog niza.

**A8.** Rekonstrukcija dela generisanog niza pseudoslučajnih brojeva korišćenjem nekog drugog njegovog dela (predikcija generisanog niza pseudoslučajnih brojeva na osnovu poznatog odsečka).

**A9.** Rekonstrukcija elemenata algoritma na osnovu dela generisanog niza pseudoslučajnih brojeva.

Dizajner kriptografskog algoritma teži da dizajnira algoritam otporan na prethodno navedene napade i da napadaču ne pruži bolji način za napad od potpune pretrage po skupu svih mogućih ključeva. Da bi to postigao, način dizajniranja i metodologija provere kvaliteta moraju da ispunjavaju sledeće uslove:

- Mora postojati spisak karakteristika algoritma koje utiču na bezbednost i o kojima se mora voditi računa prilikom dizajna kriptografskog algoritma.
- Mora postojati precizan spisak provera kojima se evaluira kvalitet kriptografskog algoritma i uputstvo za njihovo sprovođenje.
- Mora biti jasno i precizno definisano koji je minimalni skup uslova i provera navedenih u metodologiji dovoljan da bi se kriptografski algoritam smatrao bezbednim.
- Metodologija mora biti koncipirana i implementirana u formi otvorene platforme kako bi se u skladu sa proširivanjem znanja i tehnološkim napretkom mogla unapređivati

### 2.6.2 Karakteristike pseudoslučajnih generatora koje utiču na bezbednosni kvalitet

Kao što je navedeno na početku svaki sekvencijalni kriptografski algoritam šifrovanja se može posmatrati kao algoritam koji proizvodi niz pseudoslučajnih brojeva. Shodno tome svaki napad na sekvencijalni algoritam šifrovanja može se posmatrati kao napad na sekvencijalni algoritam šifrovanja koji je zasnovan na generatoru pseudoslučajnih brojeva i on se uvek bazira, osim napada potpunom pretragom po skupu svih mogućih ključeva, na nekoj karakteristici šifrata/algoritma koja sa bezbednosnog stanovišta ima loše ponašanje. Stoga je od samog početka dizajniranja algoritma šifrovanja neophodno pažljivo pristupiti izboru koncepcije algoritma i izboru njegovih gradivnih blokova.

Već u toj fazi treba voditi računa da sledeće karakteristike budu ispunjene, ako ih je moguće u tom trenutku proceniti, u skladu sa stavovima navedenim u [11, 15, 47, 65–70]:

1. Entropija ključa šifrovanja mora biti maksimalna
2. Verovatnoća ponavljanja ključa šifrovanja mora biti bliska nuli;

3. Period generisanog niza pseudoslučajnih brojeva mora biti veliki i mora biti dokazivo veći od dužine najduže poruke koja se šifruje;
4. Veličina linearne složenosti generisanog niza pseudoslučajnih brojeva mora biti što veća;
5. Profil linearne složenosti generisanog niza pseudoslučajnih brojeva bi trebalo da nema velikih oscilacija;
6. k-linearne složenosti generisanog niza pseudoslučajnih brojeva za manje vrednosti broja k ne bi trebalo da imaju velike oscilacije;
7. Algebarski stepen funkcionalnih blokova treba da bude što veći i sigurno veći od jedan;
8. Stepen nelinearnosti funkcionalnih blokova treba da bude što veći
9. Za primenjene Bulove funkcije korelaciona imunost treba da bude balansirana u odnosu na njen algebarski stepen
10. Mora biti primenjen princip konfuzije
11. Mora biti primenjen princip difuzije
12. Statističke osobine generisanog niza pseudoslučajnih brojeva moraju biti takve da ne postoje sistematska odstupanja u odnosu na osobine slučajnih nizova;
13. Moraju biti zadovoljeni lavinski efekat i striktni lavinski efekat

Navedeni zahtevi predstavljaju potrebne uslove za bezbednost algoritma šifrovanja ali ne i dovoljne. Prethodna lista je nastala kao odgovor na do sada prepoznate tehnike za napad na ovaj tip algoritama šifrovanja i stoga je neophodno kontinuirano pratiti dešavanja u ovoj oblasti kako bi se na vreme prepoznao značajan napredak u kriptoanalizi izazvan novim tehnikama kriptoanalize ili tehnološkim napretkom.

### 2.6.3 Metodologija provere kvaliteta generatora pseudoslučajnih brojeva

Po završetku dizajniranja generatora pseudoslučajnih brojeva sledi faza njegove evaluacije u bezbednosnom smislu. Teorijski, najkompletnija provera bi bila implementacija svih relevantnih napada poznatih u literaturi i u skladu sa dobijenim rezultatima oceniti definisani generator pseudoslučajnog niza. Ovakv pristup je neefikasan po više parametara. Zahteva opremu enormnih performansi (procesorska snaga i memorija), vreme za sprovođenje ovakvog tipa testiranja nije na raspolaganju i velika većina testova se ne bi završila nekim decidnim rezultatom. Zbog toga je bolji pristup da se evaluacija odvija kroz realizaciju skupa efikasnih provera čiji rezultati direktno ili indirektno ukazuju na ispunjenost/neispunjenost bezbednosnih zahteva prema definisanom generator pseudoslučajnih brojeva.

U tom smislu relavantnim proverama se smatraju:

**C1.** Ispitivanje neodređenosti početnih uslova generatora, kada se poznaje generisani niz pseudoslučajnih brojeva. Ova ispitivanja se mogu realizovati na teorijskom nivou, analizom uslovne entropije ključa kada je poznat izlazni niz iz generatora pseudoslučajnih brojeva ili eksperimentalnom statističkom analizom korelacione zavisnosti ključa i izlaznog niza iz generatora pseudoslučajnih brojeva. Način sprovođenja ove provere detaljno je opisan u [15] i [67]. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A1, A2 i A8 date u delu 2.6.1 .

**C2.** Ispitivanje verovatnoće ponavljanja ključa za šifrovanje. Ova provera je teorijska i sprovodi se u skladu sa pretpostavljenom statistikom saobraćaja korišćenjem tehnike rođendanskog problema, videti [15], poglavlje 2.1.5, strana 53. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaj A4.

**C3.** Ispitivanje stepena nelinearnosti generisanog niza pseudoslučajnih brojeva i njegove zavisnosti od ključa. Ispitivanje stepena nelinearnosti sprovodi se određivanjem stepena nelinearnosti Bulove funkcije koja je ekvivalentna generatoru. Ako nije moguće dobiti takvu ekvivalentnu reprezentaciju, zbog tehničkih ili teorijskih ograničenja, onda se gradivni blokovi algoritma predstavljaju u toj formi, analiziraju se namenski razvijenim programima i potom se na osnovu tako dobijenih rezultata analizira stepen nelinearnosti definisanog generatora. Detaljan opis stepena nelinearnosti, njegove osobine

i određivanje dati su u [42], poglavlja 2 i 6, i [21] [44] poglavlje 6. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A1, A2, A5, A6, A7, i A8 date u delu 2.6.1.

**C4.** Ispitivanje veličine perioda generisanog niza pseudoslučajnih brojeva, kao i nizova unutar generatora. Ova provera se sprovodi teorijskom analizom definisanog generatora. U slučaju da nije moguće dobiti tačnu vrednost perioda izvodi se njegova donja granica. Primeri određivanja perioda za neke tipove kriptografskih algoritama dati su u [15] u odeljku 6.3. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A3, A7 i A8 date u delu 2.6.1.

**C5.** Ispitivanje veličine linearne složenosti generisanog niza pseudoslučajnih brojeva, kao i nizova unutar generatora. Ova karakteristika se teorijski ispituje tako što se sprovodi teorijska analiza linearne složenosti gradivnih blokova algoritma a potom se izvode zaključci o linearnoj složenosti celine. Eksperimentalno se ova karakteristika ispituje primenom statističkih testova linearne složenosti na odsečcima izabranih nizova primenom Berlekamp-Mesijevog algoritma, za opis videti [15], odeljak 6.2.3.. U skladu sa dobijenim rezultatima donosi se ocena o zadovoljenosti ovog uslova. Definicija linearne složenosti i detaljne karakteristike mogu se naći u [15], odeljak 6.2.2., za matematičku analizu navedenih osobina i posledica videti [67]. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A2, A7 i A8 date u delu 2.6.1.

**C6.** Teorijsko i eksperimentalno ispitivanje statističkih osobina generisanog niza pseudoslučajnih brojeva, kao i nizova unutar generatora. Ova karakteristika se analizira teorijskom statističkom analizom i eksperimentalnom statističkom analizom primenom postojećeg okruženja za tu namenu. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A6, A7 i A8date u delu 2.6.1 .

**C7.** Teorijsko i eksperimentalno ispitivanje zavisnosti odsečaka generisanog niza pseudoslučajnih brojeva, kao i nizova unutar generatora od simbola ključa. Ova provera se sprovodi tako što se posmatra za koliko se razlikuju izlazni nizovi kada se ključevi razlikuju za jedan bit, avalanš efekat. Provera se sprovodi za svaki bit ključa. Detaljno teorijsko objašnjenje se može naći u

[42], poglavlje 3, i [44], odeljci 8.3, 8.4 i 8.5. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A1, A3 i A6 date u delu 2.6.1.

**C8.** Teorijsko i eksperimentalno ispitivanje korelacionih osobina generisanog niza pseudoslučajnih brojeva, teorijsko i eksperimentalno ispitivanje korelacionih osobina relevantnih nizova unutar generator pseudoslučajnih brojeva Ova provera se sprovodi primenom postojećeg paketa za statističko testiranje i teorijskom analizom statističkih osobina definisanog generator pseudoslučajnih brojeva. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A1, A3, A6, A7 i A8 date u delu 2.6.1.

**C9.** Teorijsko ispitivanja algebarskih karakteristika generatora pseudoslučajnih brojeva. Ova provera se sprovodi tako što se definisan generator pseudoslučajnih brojeva predstavi skupom algebarskih jednačina koji je ekvivalentan definisanom generatoru. Potom se razmatra mogućnost rešavanja tako dobijenog sistema jednačina. U zavisnosti od tipa dobijenog sistema jednačina primenjuju se odgovarajuće tehnike za njegovo rešavanje. Trenutno su aktuelne tehnike vezane za aparat komutativne algebre i Grobnerove baze. Neki aspekti ove vrste provere zahtevaju specijalizovani softver za algebarsku analizu i simboličku algebarsku analizu. Rezultati ove provere primenjuju se pri oceni osetljivosti na pokušaje A2.

U sledećoj tabeli dat je pregled napada i provera koje su relevantne za procenu mogućnosti realizacije tih napada.

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 |
|---|---|---|---|---|---|---|---|---|---|
| C1 | E,T | E,T | | | | | | | |
| C2 | | | | T | | | | | |
| C3 | T | T | | | T | T | T | T | T |
| C4 | | | T | | | | T | T | |
| C5 | | E,T | | | E,T | | E,T | E,T | E,T |
| C6 | | | | | | E,T | E,T | E,T | |
| C7 | E,T | | E,T | | | E,T | | | |
| C8 | E,T | | E,T | | | E,T | E,T | E,T | E,T |
| C9 | | E,T | | | | | | | |

Tabela 2.1: Pregled povezanosti provera i napada

Provere definisane kao teorijske sprovode, obeležene sa T u tabeli 2.1, se izvođenjem dokaza u vezi sa analiziranom karakteristikom generator pseudoslučajnih

brojeva primenom aparature neke od prethodno navedenih teorija. Provere navedene kao eksperimentalne obeležene sa E u tabeli 2.1, sprovode se izvršavanjem odgovarajućih programa. Definisane provere se obavezno sprovode u celosti. U slučaju da neke provere nije moguće sprovesti treba obrazložiti nemogućnost njihovog sprovođenja. O sprovedenom ispitivanju obavezno se sačinjava izveštaj koji sadrži opis sprovedenih ispitivanja, njihove rezultate i izvedene zaključke. Sprovedene provere, od C1 do C9, obuhvataju sve do sada poznate tipove napada na generatore pseudoslučajnih brojeva. Pozitivni rezultati ovih provera predstavljaju osnov za zaključak o praktičnoj sigurnosti algoritma šifrovanja na bazi definisanog generatora pseudoslučajnih brojeva u skladu sa aparaturom i metodologijom teorije složenosti izračunavanja. Pozitivni rezultati ovih provera ne predstavljaju garanciju njegove apsolutne bezbednosti u smislu teorije informacija.

Imajući u vidu prethodno konstatovanu činjenicu da skup bezbednosnih zahteva prema definisanom generatoru pseudoslučajnih brojeva predstavlja u suštini skup potrebnih uslova, u slučaju da bilo koja provera da negativan bezbednosni rezultat smatra se da generator ne ispunjava bezbednosne uslove i da ukoliko je to moguće, treba redefinisat generator . Ovakav stav je potkrepljen činjenicom da su provere i zahtevi definisani na osnovu mogućnosti izvođenja uspešnog napada na generator pseudoslučajnih brojeva u slučaju neispunjenja definisanih zahteva.

# Glava 3

# Sekvencijalni kriptografski algoritmi sa promenljivim permutacijama

Značajnu klasu kriptografskih algoritama u simetričnoj kriptografiji čine sekvencijalni kriptografski algoritmi. Po bezbednosnim karakteristikama sekvencijalni kriptografski algoritmi spadaju u praktično sigurne šifarske sisteme. Strukturno gledano sekvencijalni kriptografski algoritmi su dominantno realizovani kao binarni pseudoslučajni generatori čiji se elementi izlaznog niza sabiraju po modulu dva sa elementima poruke koja se štiti i na taj način formiraju simbole šifrata. Tri su osnovne osobine ovakvih konstrukcija:

1. To su deterministički algoritmi koji na osnovu relativno kratke slučajne vrednosti $k$, nekoliko stotina bita, generišu niz izlaznih simbola koji je i za nekoliko desetina redova veličine duži od dužine slučajne vrednosti $k$. Ova osobina omogućava da se ovakvim sistemom mogu štiti poruke proizvoljne dužine.

2. Po svojoj matematičkoj prirodi pseudoslučajni generatori su konačni automati sa izlazom i prema tome izlazni niz koji generišu je periodičan. Posledica ove periodičnosti je da dužina poruke koja se štiti mora biti manja od dužine perioda generatora, zahtev kriptografske bezbednosti. U suprotnom bezbednost štićene poruke bi bila ugrožena, [50], [51].

3. Sigurnosni parametar $n$ koji predstavlja dužinu kriptografskog ključa $k$ je bitan parametar bezbednosti ove klase kriptografskih algoritama. Inherentna

slabost ove konstrukcije je napad grubom silom, pretraga po skupu svih mogućih ključeva, i stoga odabrana dužina mora biti takva da taj napad čini efektivno neizvodljivim.

Postoji više tehnika za sintezu pseudoslučajnih generatora, videti odeljak 2.3 na strani 17. U ovom delu detaljnije ćemo se baviti primenom promenljivih permutacija u sintezi sekvencijalnih kriptografskih algoritama.

Kvalitet sigurnosnih rešenja u sajber prostoru u osnovi se izražava sa dva parametra, stepenom bezbednosti i efikasnošću izvršavanja koja podrazumeva zahtev da bezbednosna rešenja ne narušavaju komunikacione karakteristike sistema. Pseudoslučajni generator RC4 je izuzetno efikasna i ekonomična konstrukcija bazirana na promenljivim permutacijama. Ideja promenljivih permutacija sastoji se u tome da permutacija bude deo unutrašnjeg stanja pseudoslučajnog generatora kada se ovaj posmatra kao konačni automat i da se sa promenom unutrašnjeg stanja konačnog automata i ona menja. U svojoj osnovnoj realizaciji pseudoslučajni generator RC4 je izuzetno jednostavan a lepota i elegancija te ideje pospešile su njenu eksploataciju. Pojavilo se više konstrukcija sa pokušajima primene promenljivih permutacija. Neke od njih su kriptografski algoritam Py, [71], kriptografski algoritam MV3, [72], kriptografski algoritam HC-256, [73]. Bezbednosne analize opisane u radovima [74–77] su pokazale izvesne slabosti navedenih kriptografskih algoritama . Pomenute slabosti su uticale da se navedeni kriptografski algoritmi ne svrstaju u kategoriju algoritma koji se preporučuju za upotrebu u bezbednosnim rešenjima.

## 3.1 Generator pseudoslučajnih brojeva RC4

Ideja upotrebe promenljivih permutacija u sintezi generatora pseudoslučajnih brojeva pojavila se prvi put u radu Marasalje i Maklarena, [78]. U toj realizaciji postoji velika tabela koja se sa vremenom rada generatora polako menja a promene su determinisane stanjima generatora i izlaznim nizom po vremenu rada. Realizovana ideja svoju popularnost duguje jednostavnosti, efikasnosti i lakoći implementacije mada nije lako teorijski utvrditi statističke osobine ovakvih generatora.

Koristeći tu ideju Ronald Rajvest je 1987 godine za potrebe kompanije RSA Data Security kreirao pseudoslučajni generator RC4. Kompanija je pseudoslučajni generator RC4 koristila u svojim bezbednosnim rešenjima. Opis generatora

nije bio javno dostupan i čuvan je kao poslovna tajna. Na Internetu se anonimno pojavio opis ovog algoritma 1994. godine i tokom vremena je verifikovana njegova verodostojnost reverznim inženjeringom bezbednosnih rešenja kompanije RSA Data Security. Verodostojnost dobijenog opisa potvrdio je sam Rajvest u [79], [80]

### 3.1.1 Opis generatora pseudoslučajnih brojeva RC4

U apstraktnom smislu pseudoslučajni generator RC4 se sastoji od tabele koja sadrži sve elemente dužine $n$ bita, ukupno njih $N = 2^n$, i dva $n-$ bitna indeksa koji se koriste za adresiranje elemenata tabele. Početno stanje pseudoslučajnog generatora RC4 se određuje na osnovu odabranog ključa $k$. Dužina ključa se određuje pri definisanju bezbednosnog rešenja. Unutrašnje stanje pseudoslučajnog generatora RC4 čini uređena trojka koju čine tabela i dva pomenuta indeksa. U konkretnoj realizaciji pseudoslučajnog generatora RC4 izabrano je $n = 8$. Uobičajeno je da se tabela označava sa $S$ a indeksi sa $i$ i $j$.

#### 3.1.1.1 Algoritam definisanja početnog stanja pseudoslučajnog generatora RC4

Početno stanje pseudoslučajnog generatora RC4 se formira upotrebom ključa $k = \{k_l\}_{l=1}^{m}$ i tabele $S[l] = l,\ l = 0, 1, 2, ..., 255$. Inicijalna vrednost tabele je takva da predstavlja jediničnu permutaciju. Postupak inicijalizacije pseudoslučajnog generatora RC4, definisanje početnog stanja konačnog automata, se u literaturi označava sa KSA (Key Scheduling Algorithm).

Definisanje početnog stanja za konačni automat koji odgovara pseudoslučajnom generatoru RC4 se sprovodi prema sledećem algoritmu:

1. $S[l] = l,\ l = 0, 1, 2, ..., 255$
2. $S, \{k_i\}_{i=1}^{l}, i = 0,\ j = 0, K_i$
3. Da li je $i > 255$, ako „ne" pređi na 5, ako „da" pređi na 9.
4. $K[i] = k[i \bmod l]$
5. $j = j + S[i] + K[i]$
6. Zameni sadržaj mesta u permutaciji $S$ na pozicijama $i$, i $j$ $S[i] \longleftrightarrow S[j]$
7. $i = i + 1$

8. Vrati se na 3.

9. Kraj

i njegov pseudo-kod:

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

Uloga ove procedure je da se koristeći ključ $k$ počevši od jedinične permutacije generiše nova, neprediktabilna, permutacija koja će se koristiti u generisanju prvog elementa izlaznog niza pseudoslučajnog generatora RC4 i dalje se menjati u toku rada prema definisanom pravilu u algoritmu. Ovim se postiže da se ne zna unapred permutacija sa kojom generisanje elemenata pseudoslučajnog generatora počinje. U praksi se koriste dužine ključa $k$ između 80 i 256 bita.

#### 3.1.1.2 Algoritam generisanja elemenata izlaznog niza pseudoslučajnog generatora RC4

Na početku ovog procesa permutacija $S$ ima vrednost koju je dobila posle završetka KSA procesa. Izlazni niz ćemo označiti sa $Z$. Postupak generisanja izlaznog niza $Z$ pseudoslučajnog generatora RC4, u oznaci PRGA (Pseudo Random Generator Algorithm), se odvija na sledeći način:

1. Stavimo $S$ iz KSA i $i = 0$, $j = 0$,
2. $i = (i + 1) \bmod 256$
3. $j = (j + S[i]) \bmod 256$
4. Zameni sadržaj mesta u permutaciji $S$ na pozicijama $i$, i $j$ $S[i] \longleftrightarrow S[j]$
5. $Z = (S[S[i] + S[j]]) \bmod 256$

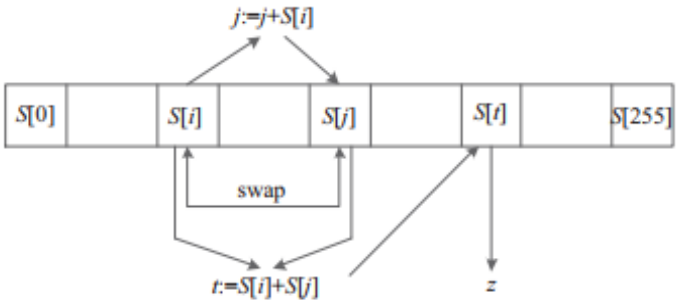
6. Izlaz $Z$

7. Vrati se na 2.

i njegov pseudo-kod:

```
i := 0 j := 0
while GeneratingOutput:
    i := (i + 1) mod 256;
    j := (j + S[i]) mod 256;
    swap values of S[i] and S[j];
    Z := S[(S[i] + S[j]) mod 256] output Z;
endwhile.
```

Na sledećoj slici je grafički prikaz rada RC4 algoritma preuzet iz []:




Slika 3.1: GrafiÄŤki prikaz generisanja izlaznog niza pseudosluÄŤajnog generatora RC4

Pseudoslučajni generator RC4 je jedan od najeksploatisanijih pseudoslučajnih generatora i primenjuje se ili se primenjivao u mnogim protokolima kao što su : Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) protokolu, BitTorrent protokolu, Microsoft Office XP, Microsoft Point-to-Point Encryption, Transport Layer Security/Secure Sockets Layer,Secure Shell, Remote Desktop Protocol, Kerberos, SASL Mechanism Digest-MD5, Gpcode.AK, Skype.

## 3.2 Bezbednosne karakteristike pseudoslučajnog generatora RC4

Bezbednost pseudoslučajnog generatora RC4 se procenjuje u okviru klase praktično sigurnih kriptografskih algoritama. Kao i za većinu algoritama toga tipa u praksi se primenjuje model složenosti izvršavanja opisan u delu 2.4.4 na strani 49. U tom kontekstu ciljevi kriptoanalize mogu biti raznoliki, od potpune kompromitacije sistema kada napadač može da sazna sadržaj poruke bez poznavanja ključa do pokušaja da se konstruiše raspoznavač koji je u stanju da izlaznu sekvencu analiziranog generatora razlikuje od slučajnog niza sa verovatnoćom bliskom jedinici. U definisanju ciljeva kriptoanalize veliku ulogu igra i eksperimentalna analiza nad izlaznim nizovima generatora jer neretko ti rezultati ukazuju na slabosti koje se potom teorijski obrađuju i klasifikuju.

Pseudoslučajni generator RC4 je zbog svoje popularnosti i masovne upotrebe bio predmet brojnih detaljnih ispitivanja u pogledu kriptografskih osobina. Analize se mogu grubo govoreći svrstati u tri grupe:

- U odnosu na kriptografske ključeve što obuhvata uticaj primenjenog kriptografskog ključa na izlazni niz i prelivanje informacija o bitima ključa i njihovom odnosu u izlazni niz.

- U odnosu na unutrašnje stanje konačnog automata koji odgovara generatoru RC4 što obuhvata prelivanje informacija o unutrašnjem stanju u izlazni niz.

- U odnosu na statistička i korelaciona svojstva izlaznog niza.

Dobijeni su brojni rezultati o slabostima ovog algoritma. Jedan deo napada je kreiran heuristički na osnovu rezultata eksperimentalnih ispitivanja dok je drugi deo napada formalno teorijski utemeljen. Da bi se prikazali rezultati pomenutih ispitivanja uvode se sledće oznake i pretpostavke.

Kao što je objašnjeno u delu 2.2.1 pod taktom ćemo podrazumevati računanje jednog elementa pseudoslučajnog niza. Dakle, element $z_i$ izlaznog niza $Z$ se izračunava u $i-$tom taktu. Unutrašnje stanje generatora RC4 određeno je sadržajem permutacije $S$, i vrednostima indeksa $i, j$ u oznaci $(S, i, j)$. Neka nam $r$ označava redni broj takta, $r = 1, 2, 3, \ldots$. Stanje pseudoslučajnog generatora RC4 u $r-$tom taktu označićemo sa $(S_r, i_r, j_r)$ gde je $S_r$ permutacija koja se dobija transformacijom permutacije $S_{r-1}$. Dalje, označimo sa $t_r = (S_r[i_r] + S_r[j_r]) \bmod 256$

vrednost adrese izlaznog bajta u $S_r$, a izlazni bajt pseudoslučajnog generatora sa $z_r = S_r[t_r]$. Da bi se razlikovale oznake u fazama KSA i PRGA u $r-$tom taktu promenljive u KSA algoritmu kojima se opsuje tekuće stanje imaće u eksponentu oznaku $K$. Aritmetičke operacije se odnose na modularnu aritmetiku po modulu 256.

### 3.2.1 Analiza uticaja ključeva na početno stanje generatora

Uloga ključa $k$ u formiranju početnog stanja pseudoslučajnog generatora RC4 je da početno stanje bude neprediktabilno. Stanje pseudoslučajnog generatora RC4 je $(S, i, j)$. Veličina prostora stanja je za skup svih mogućih tabela $S$ je data sa

$$256! \approx 2^{1684}$$

i algoritmom KSA kao početno stanje izračunava jedno od njih a potom se algoritmom PRGA generiše izlazni niz. Ovaj tip analiza se bavi prepoznavanjem postojanja veza između primenjenog ključa i odabranog početnog stanja sa ciljem rekonstrukcije ključa ili nekih njegovih delova poznavanjem izlaznog niza.

#### 3.2.1.1 Uticaj različitih ključeva na izlazni niz generatora RC4

Jedno od prvih pitanja koje se nameće je da li se može desiti da dva različita ključa $k_1$ i $k_2$ dovode generator RC4 u isto početno stanje što dovodi do toga da su im generisani izlazni nizovi jednaki. Činjenica je da je egzistencija takvih stanja uslovljena dužinom ključeva. To se lako vidi kada su ključevi takvi da je $|k| > 1700$ bita jer tada skup početnih stanja ima manji broj elemenata od skupa ključeva i korespondencija ne može biti jednoznačna. Cilj je da se utvrdi da li je prethodna situacija moguća u slučaju ključeva čija je dužina manja od 1700 bita i ako jeste kako se mogu takvi ključevi konstruisati.

**Definicija 13** *Neka su $k_1$ i $k_2$ dva različita ključa i neka su $S^1$ i $S^2$ vrednosti permutacije po završetku KSA algoritma. Ako je $S^1 = S^2$ tada za ključeve $k_1$ i $k_2$ kažemo da su povezani.*

Nešto slabiji zahtev, da se $S^1$ i $S^2$ na kraju KSA procesa razlikuju za malo i da u nekom početnom delu generisani nizovi budu jednaki rešili su u svom radu iz 2000

godine Grosul i Valah. Oni su konstruisali par ključeva tako što su odabrali ključ $k_1$, a ključ $k_2$ se dobija iz $k_1$ komplementiranjem na pozicijama koje ne narušavaju proces tranzicije stanja tako da su se izlazni nizovi poklapali na oko sto prvih bajtova. Za potpune informacije videti [81].

Detaljan odgovor na pitanja koja proističu iz definicije 13 dao je Matsui u svom radu [82]. Pokazao je da ako ključevi $k^1$ i $k^2$ zadovoljavaju sledeće relacije

$$\begin{aligned} \left|k^1\right| &= \left|k^2\right| = m, \\ k_i^1 &= k_i^2 \qquad\qquad i \neq d \\ k_i^1 &= k_i^2 - 1 \qquad i = d \\ 0 &\leq d < m \end{aligned}$$

za $i = 0, 1, ..., m-1$ a broj $n$ je dat sa $n = \left\lfloor \frac{256+m-1-d}{m} \right\rfloor$. Verovatnoća da će na kraju KSA faze tabele permutacija bit jednake data je sa

$$P\left(S^1 = S^2\right) = \begin{cases} \left(\frac{254}{256}\right)^d \left(\frac{255}{256}\right)^{(n-1)(m-2)-2} \left(\frac{1}{256}\right)^{n+2} & d \neq m-1 \\ \left(\frac{254}{256}\right)^{d-1} \left(\frac{255}{256}\right)^{(n-1)(m-2)-2} \left(\frac{1}{256}\right)^{n+2} & d = m-1 \end{cases}$$

odnosno

$$P\left(S^1 = S^2\right) \approx \frac{1}{e} \cdot \left(\frac{1}{256}\right)^{n+2}.$$

U istom radu Matsui je uspeo da konstruiše ključeve dužine 176 bita.

Sličan pokušaj su realizovali Biham i Dankelman primenjujući tehnike diferencijalne kriptoanalize, videti [83].

#### 3.2.1.2 Otkrivanje kriptografskog ključa uz poznato unutrašnje stanje generatora RC4

Pseudoslučajni generator RC4 je po svojoj prirodi deterministički automat sa karakteristikom da ako se poznaje $z_r$ i $(S_r, i_r, j_r)$ tada je lako rekonstruisati prethodno stanje $(S_{r-1}, i_{r-1}, j_{r-1})$. na taj način se lako dolazi do vrednosti $S_0$ koja je rezultat KSA algoritma. Da bi se došlo do vrednosti ključa mora se naći invertibilna funkcija za KSA proces u čemu prethodni postupak nije od pomoći jer KSA proces ne produkuje izlazne vrednosti.

Za problem invertibilne transformacije u odnosu na KSA dugo nije bilo rešenja dok Paul i Maitra nisu 2007. publikovali rad u kojem je objavljeno rešenje ovog

problema, [84]. Koristeći eksperimentalno potvrđenu činjenicu da postoji korelacija između prvih nekoliko bajtova izlaznog niza i bajtova ključa, [85] definisali su sistem jednačina po modulu 256 koji je uz poznavanje $S_0$ efikasno rešiv.

Drugačije i efikasnije rešenje zasnovano na tehnikama diferencijalne kriptoanalize publikovali su Biham i Kameli [86].

Analizirajući KSA algoritam u radu [87] Agun, Kavak i Demir, su došli do novih statističkih karakteristika KSA algoritma i njihovom primenom definisali efikasniji algoritam za otkrivanje ključa.

Oslanjajući se na ideje iz [86] ali primenjujući ih za rekonstrukciju pojedinačnih bita ključa umesto bajtova Kazei i Meir su u [88] dobili efikasniji algoritam za rešavanje ovog problema.

#### 3.2.1.3 Otkrivanje kriptografskog ključa na osnovu poznavanja izlaznog niza generatora RC4

Otkrivanje mogućnosti za rekonstrukcija ključa na osnovu poznavanja generisane pseudoslučajne sekvence predstavlja tip napada CPA opisan na strani 34.

Efikasnost u produkcionom, eksploatacionom i implementacionom smislu učinili su da pseudoslučajni generator RC4 bud odabran kao deo kriptografskog okruženja u standardu WEP protokolu koji se upotrebljava za zaštitu komunikacija u Wi-Fi IEEE 801.11.LAN mrežama. Taj izbor ga je automatski postavio u fokus kriptoanalitičarske zajednice čime postaje predmet masovnih i detaljnih analiza. Tako veliki i skoncentrisan istraživački napor urodio je plodom i ubrzo su se pojavili rezultati koji su omogućili kreiranje uspešnih napada na WEP protokol kada koristi RC4 generator. U apstraktnom smislu scenario napada je sledeći. Napadač na neki način dolazi u posed šifrata i njemu odgovarajućih poruka kao i inicijalnog vektora koji protokol koristi. U današnjim telekomunikacijama formiranje ovakvog skupa podataka se može smatrati relativno rutinskom procedurom. Parovi (poruka, šifrat) služe da se otkrije izlazni niz iz generatora RC4 a zatim se nekim od objavljenih napada uz poznavanje inicijalnog vektora dobija primenjeni ključ. Uspešni napadi ovog tipa su brojni i zarad informativnosti nabrojaćemo neke od njih ali ih nećemo objašnjavati i komentarisati: Flurer, Mantin i Šamir (FMS) napad [89]; Korekov napad [90], [91]; Mantinovi napadi na RC4 i WEP [92]; Klienov napad [93]; Tevsov, Veinmanov i Piškinov (TWP) napad [94]; Vaudenov i Vuaganov napad [95]; Tevsov i Bekov napad [96], Šeperdov, Vaudenov i Vuauganov napad [97]; Šeperdov, Vaudenov i Vuauganov napad [98] i Šeperdov napad [99].

Ove analize i na njima zasnovani u praksi uspešni napadi doveli su do toga da se upotreba RC4 generatora u bezbednosnim rešenjima ne preporučuje, [100].

Kao zamena za WEP protokol definisan je WPA protokol koji takođe koristi RC4 kriptografsko obezbeđenje. Dizajn WPA protokola rukovodio se ciljem izbegavanja poznatih napada na WEP protokol. Na žalost, pokazalo se da i je i on ugrožen napadima [94], [98].

Protokol WPA je zamenjen protokolom WPA2 koji se u svom kriptografskom repertoaru oslanja na algoritam AES.

Ovde treba napomenuti da katastrofalne bezbednosne karakteristike WEP i WPA protokola nisu isključiva posledica slabosti RC4 algoritma već bi se pre moglo konstatovati da je to posledica neadekvatnog izbora i sprezanja protokola, kriptografskog algoritma i kriptografskih parametara.

#### 3.2.1.4 Korelacione osobine ključeva

Indikacije za većinu slabosti generatora RC4 pojavile su se kao rezultat eksperimentalnih analiza. Tako je A. Ros eksperimentalnom analizom uočio da postoji značjna verovatnoća da vrednost prvog bajta izlaznog niza generisanog generatorom RC4 bude $z_1 = k_2 + 3$ za ključ $k_0, k_1, ...., k_{l-1}$ gde važi $k_0 + k_1 = 0$. Njegova eksperimentalna analiza je pokazala da je verovatnoća ovog događaja između 0.12 i 0.16, videti [85]. Kasnije su ovi rezultati potvrđeni i teorijski, videti [84].

U [102] potvrđena je veza između prva dva elementa permutacije $S$ i prva dva bajta ključa.

**Teorema 14** *[102] Posle KSA algoritma najveća verovatnoća za sadržaje pozicija* $S[1], S[2]$ *data je sa*

1. $P(S_N^0[1] = k_0 + k_1 + 1) \approx \left(\frac{N-1}{N}\right)^N$
2. $P(S_N^0[2] = k_0 + k_1 + k_2 + 3) \approx \left(\frac{N-1}{N}\right)^N$

### 3.2.2 Otkrivanje unutrašnjeg stanja generatora RC4 na osnovu odsečka generisanog niza

U 3.2.1.2 na strani 69 je konstatovano da je PRGA RC4 invertibilna funkcija uz poznavanje tekućeg unutrašnjeg stanja i izlaznog bajta. Stoga se jedan deo

istraživača usredsredio na pokušaje da analizom izlaznog niza pokuša da rekonstruiše unutrašnje stanje generatora a potom dođe do upotrebljenog kriptografskog ključa.

U literaturi se često navodi sledeća računica o broju svih mogućih unutrašnjih stanja RC4 algoritma

Kao što smo ranije rekli, unutrašnje stanje pseudoslučajnog generatora RC4 je definisano permutacijom $S$ i indeksima $i, j$. Prostor stanja čine uređenje trojke $(S, i, j)$ gde indeksi $i, j \in \{0, 1, 2, ...., N-1\}$ a $S$ je permutacija reda $N$. Skup koji sadrži sve takve trojke ima ukupno

$$|\{(i, j, S)\,|i, j \in \{0, 1, 2, ...., N-1\} \wedge S \text{ je permutacija reda } N\}| = N \cdot N \cdot N!$$

članova. Kako je kod pseudoslučajnog generatora RC4 $N = 256$ ukupan broj stanja je jednak

$$256^2 \cdot 256! = 2^{16} \cdot 256! \approx 2^{16} \cdot 2^{1684} = 2^{1700}$$

Za prostor stanja ove veličine bi se očekivalo da ne postoje efikasni načini pretrage i otkrivanja tekućeg stanja pseudoslučajnog generatora RC4. Međutim, pokazalo se da nije tako. Vremenom se pojavio čitav niz algoritama napada koji su smanjivali veličinu prostora pretrage i činili je značajno manjom u odnosu na veličinu polaznog prostora.

Prvi prodor načinili su 1998 godine Knudsena, Mejera i Prenela u radu [103]. Njihov napad za vrednost $N = 256$ ima složenost $2^{779}$.

Analizirajući situaciju kada je permutacija reda $N = 32$, Mister i Tavares su koristeći cikličnu dekompoziciju RC4 algoritma definisali napad čija je složenost $2^{42}$, [104].

Nešto drugačiji pristup demonstrirali su Golić i Morgari u [105] gde su stohastičkim rekurzivnim metodama formulisali napad sa složenošću $2^{689}$, [105].

Ideje o rešavanju ovog problema su evoluirale pa se krenulo u razmatranje situacija kada je jedan deo pozicija permutacije $S$ poznat. Širaiši, Ohigaši, i Mori su u radu [106] analizirali situaciju kada je poznat sadržaj 112 pozicija permutacije $S$ i dobili napad složenosti $2^{220}$. Daljom analizom su uspeli da redukuju neophodan broj poznatih pozicija na 73 sa sličnom složenošću.

Naslanjajući se na ideje iz [103] Tomašević, Bojanić i Nieto-Talandez su nizom poboljšanja i optimizacija u procesu pretrage definisali napad čija je složenost $2^{739}$, [107]

Koristeći sličan pristup kao u [106] Maksimov i Khovratovich su definisali napad koji rekurzivnim metodama pretrage rekonstruiše unutrašnje stanje generatora sa složenošću $2^{241}$, [108].

Dodatna poboljšanja postigli su Golić i Morgari definišući napad sa složenošću $2^{211}$, [105].

Navedeni rezultati pokazuju značajan napredak u rešavanju problema rekonstrukcije unutrašnjeg stanja pseudoslučajnog generatora RC4 sa $2^{1700}$ na $2^{211}$ ali ti napadi su još uvek daleko od operativne upotrebljivosti.

### 3.2.3 Analiza statistički osobina generatora RC4

U delu 2.6 konstatovano je da su dobre probabilističke osobine generatora pseudoslučajnih nizova neophodan uslov njihovog kriptografskog kvaliteta i primenljivosti. To se odnosi kako na sam generisani pseudoslučajni niz tako i na nizove koji se pojavljuju unutar generatora tokom procesa generisanja izlaznog niza. Postojanje statističkih anomalija u bilo kom delu generatora predstavlja potencijalnu pretnju čija eksploatacija može dovesti do kompromitacije generatora. Inicijalni zahtev za svaki generator je da njegovi nizovi i elementi imaju uniformnu raspodelu u odnosu na skup mogućih vrednosti. Na taj način se eliminišu mogućnosti uspešne primene statističkih metoda kriptoanalize prema predmetnom generatoru. Statistička kriptoanaliza obuhvata probabilističku analizu generisane sekvence, statističku analizu elemenata unutrašnjeg stanja pseudoslučajnog generatora kao i statističku korelacionu analizu uticaja elemenata unutrašnjeg stanja pseudoslučajnog generatora na generisanu sekvencu. Poseban deo statističke analize je korelaciona analiza koja se bavi odnosom uticaja kriptografskog ključa i stanja pseudoslučajnog generatora.

Skoro svi uspešni napadi na pseudoslučajni generator RC4 rezultat su probabilističke kriptoanalize. Detekcija neuniformnih raspodela verovatnoća pojedinih elemenata algoritma kao i postojanje korelacije između elemenata unutrašnjeg stanja RC4 omogućila su uspešne napade na ovaj generator pseudoslučajnih sekvenci.

#### 3.2.3.1 Analiza raspodele unutrašnjeg stanja RC4 algoritma

Kao i u prethodnim delovima uređenu trojku $(S, i, j)$ ćemo zvati unutrašnjim stanjem generatora RC4.

Uobičajen pristup pri statističkoj analizi generatora RC4 je da se prihvata pretpostavka da pojava unutrašnjih stanja u toku rada generatora ima uniformnu raspodelu. Pokazalo se da ova pretpostavka nije korektna.

**3.2.3.1.1 Finijevi ciklusi** U teoriji konačnih automata jedan od važnih algoritama je algoritam za detekciju nedostižnih stanja automata. U slučaju pseudoslučajnog generatora RC4 ta analiza je složena zbog veličine skupa mogućih stanja ali je Finney na lucidan način uspeo da pokaže da u skupu svih stanja za generator RC4 postoje nedostižna stanja [109].

**Definicija 15** *Stanje* $(S, i, j)$ *nazivamo Finijevim ako važi:*

**1.** $j = i + 1$

**2.** $S[j] = 1$

Kako je početno stanje generatora RC4 $(S, 0, 0)$ a Finijeva stanja su regularni pripadnici prostora stanja postavlja se pitanje da li su ona dostižna iz početnog stanja.

**Teorema 16** *Neka u* $r$*-tom taktu generatora RC4 unutrašnje stanje generatora ispunjava sledeća dva uslova:*

$$\begin{aligned} j_r &= i_r + 1 \\ S_r[j_r] &= 1 \end{aligned} \tag{3.1}$$

*onda*

**( a )** *Za proizvoljno* $k \geq 1$ *je* $j_{r+k} = i_{r+k} + 1$ *i* $S_{r+k}[j_{r+k}] = 1$

**( b )** *Počevši od* $(S_r, i_r, j_r)$ *u prostoru stanja formira se ciklus dužine* $N \cdot (N-1)$

**( c )** *Izlazni bajtovi* $z_{r+(N-1)}, z_{r+2(N-1)}, z_{r+3(N-1)}, ..., z_{r+N\cdot(N-1)}$ *predstavljaju permutaciju* $S_r$.

**Dokaz.**

**( a )** Neka su u $r$-tom taktu generatora RC4 zadovoljeni uslovi teoreme 16. Tada će elementi unutrašnjeg stanja u $r+1$-om taktu imati vrednosti

$$\begin{aligned} i_{r+1} &= i_r + 1 \\ j_{r+1} &= j_r + S_r\left[i_{r+1}\right] = \\ &= i_r + 1 + 1 = \\ &= i_r + 2. \end{aligned} \tag{3.2}$$

Transformacija permutacije $S_r$ za $r+1$ takt koja koristi indekse $i_{r+1}$ i $j_{r+1}$ date u (3.2) daje

$$\begin{aligned} S_{r+1}\left[i_r + 2\right] &= 1 \\ S_{r+1}\left[i_r + 1\right] &= S_r\left[i_r + 2\right] \end{aligned} \tag{3.3}$$

Sada iz (3.3) sledi da u $(r+1)$-om taktu će generator biti u unutrašnjem stanju $(S_{r+1}, i_{r+1}, j_{r+1})$ i između njegovih elemenata važi ista relacija kao za elemente $r$-te runde

$$\begin{aligned} j_{r+1} &= i_{r+1} + 1 \\ S_{r+1}\left[j_{r+1}\right] &= 1 \end{aligned} \tag{3.4}$$

Primenjujući sada princip matematičke indukcije zaključujemo da je tvrđenje $(a)$ tačno.
Ovim smo pokazali da je relacija (3.2) invarijantna u radu generatora RC4.

**( b )** Uslov teoreme 16 znači da se generator nalazi u Finijevom stanje a kao posledicu tvrđenja $(a)$ znamo da će se ta relacija u vremenu i dalje održavati pa će se u svakoj sledećem taktu sadržaj sa pozicije $i_r+2$ pomeriti na poziciju $i_r+1$ a vrednost 1 će sa pozicije $i_r+1$ preći na poziciju $i_r+2$. Prema tome, posle $N$ taktova vrednost 1 će se u permutaciji zauzimati poziciju $i_r+1$ a ostale vrednosti će se pomeriti za po jedno mesto u levo u permutaciji $S$.Nakon $N$ ponavljanja ovog procesa u $r+N\,(N-1)$-om taktu za permutacije $S_r$ i $S_{r+N(N-1)}$ važiće

$$S_r \equiv S_{r+N\cdot(N-1)}$$

čime je postojanje ciklusa utvrđeno. Da će se kretanje po ciklusu nastaviti posledica je tvrđenja pod $(a)$.

**( c )** Koristeći se rezultatima dokaza dela $(b)$ za fiksirano $i_r$ imamo da je

$$\begin{aligned} S_r\left[i_r\right] &= S_{r+N-1}\left[i_{r+N-1}\right] \\ S_{r+k}\left[j_{r+k}\right] &= 1, \;\; k \geq 0 \end{aligned} \tag{3.5}$$

Prema tome vrednost indeksa koji adresira permutaciju je posle $N-1$ taktova, $S_{r+N-1}\left[i_{r+N-1}\right] + S_{r+N-1}\left[j_{r+N-1}\right]$, je konstantna. Ovo znači da će izlazni bajtovi generatora posle svakih $N-1$ taktova biti generisani sa iste pozicije tekuće permutacije. Zbog postojanja ciklusa u svakom krugu od $N-1$ taktova će se na toj poziciji nalaziti drugi element permutacije $S$. Otuda sledi da ce izlazni elementi čija je međusobna udaljenost $N-1$ predstavljati permutaciju $S$ čime je dokaz završen.

■

Da bi smo dokazali postojanje nedostižnih stanja neophodno je pokazati da u toku rada pseudoslučajni generator RC4 nikada ne može doći u Finijevo stanje i formirati Finijev ciklus.

**Posledica 17** *Algoritam RC4 nikada ne može formirati Finijev ciklus.*

**Dokaz.** Da bi smo ovo pokazali dovoljno je pokazati da generator RC4 ne može doći u Finijevo stanje. Dokaz ćemo izvesti polazeći od suprotne pretpostavke. Dakle neka u $r-$tom taktu algoritam dospeva u Finijevo stanje $(S_r, i_r, j_r)$ i shodno tome važi

$$\begin{aligned} j_r &= i_r + 1 \\ S_r\left[j_r\right] &= 1 \end{aligned} \tag{3.6}$$

Pokažimo sada da je i stanje $(S_{r-1}, i_{r-1}, j_{r-1})$ Finijevo.
U $r-$tom taktu po definiciji, sadržaji sa pozicija $(i_r, j_r) = (i_r, i_r + 1)$ u permutaciji $S_{r-1}$ zamene mesta i imamo da je $S_r\left(i_r + 1\right) = 1$. Iz ovoga sledi da je $S_{r-1}\left(i_r\right) = 1$ odnosno

$$S_{r-1}\left(i_r\right) = S_{r-1}\left(i_{r-1} + 1\right) = 1. \tag{3.7}$$

Po definiciji algoritma RC4 imamo

$$j_r = j_{r-1} + S_{r-1}\left(i_r\right)$$

i koristeći (3.7) i (3.6) dobijamo

$$\begin{aligned} j_r &= j_{r-1} + S_{r-1}(i_r) \\ i_r + 1 &= j_{r-1} + 1 \\ j_{r-1} &= i_r = i_{r-1} + 1. \end{aligned} \tag{3.8}$$

Iz (3.7) i (3.8) dobijamo

$$\begin{aligned} j_{r-1} &= i_{r-1} + 1 \\ S_{r-1}(j_{r-1}) &= 1 \end{aligned}$$

odakle sledi da je stanje $(S_{r-1}, i_{r-1}, j_{r-1})$ Finijevo.
Vraćajući se unazad dobijamo da je i početno stanje $(S, 0, 0)$ Finijevo što nije tačno jer ne zadovoljava uslove definicije 15.
Kako naša pretpostavka vodi do apsurda to znači da nije tačna i da generator RC4 nikada ne dolazi u Finijevo stanje. ■

Iz posledice 17 sledi da pseudoslučajni generator RC4 ne prolazi sva stanja iz prostora mogućih stanja, odnosno da dostižna stanja nemaju uniformnu raspodelu na prostoru svih mogućih stanja.

#### 3.2.3.2 Analiza probabilističkih osobina izlaznog niza pseudoslučajnog generatora RC4

Statistička analiza izlaznog niza pseudoslučajnog generatora je jedan od osnovnih pokazatelja kvaliteta generisane sekvence. Ispitivanje se može odvijati na dva koloseka, teorijskom i eksperimentalnom.

Označimo sa $\{z_i\}_{i=0}^{\infty}$ izlazni niz generatora RC4.

Teorijska statistička analiza izlaznog niza generatora RC4 obuhvata određivanje funkcije raspodele slučajne promenljive $z_i, i = 1, 2, ...$ i njenu komparaciju sa uniformnom raspodelom. U slučaju odstupanja od uniformne raspodele neophodno je odrediti njihov uzrok, veličinu i prirodu. Po prirodi ova odstupanja mogu biti:

- Bliska odstupanja, koja su prisutna na relativno kratkim početnim segmentima.

- Udaljena odstupanja čije pojavljivanje nije ograničeno na dužinu izlaznog niza, mogu se pojavljivati na proizvoljnoj udaljenosti u generisanom izlaznom nizu.

Razmatranja se odvijaju u dve faze koje korespondiraju sa fazama izvršenja pseudoslučajnog generatora. Prva faza, KSA, inicijalizacija generatora produkuje početnu vrednost permutacije $S$. U slučaju da je svaka permutacija moguća i jednako verovatna imali bi smo da je

$$P\left(S\left[u\right]=v\right)=\frac{1}{N} \qquad (3.9)$$
$$u,v\in\{0,1,\ldots,(N-1)\}$$

Raspodelu verovatnoća za permutaciju $S$ posle faze inicijalizacije odredio je Mantin u [110] i pokazao da je funkcija raspodele početne permutacije $S_0$ data sa

$$P\left(S_0\left[u\right]=v\right)=\begin{cases}\frac{1}{N}\left(\left(\frac{N-1}{N}\right)^v+\left(1-\left(\frac{N-1}{N}\right)^v\right)\left(\frac{N-1}{N}\right)^{N-u-1}\right) & v\leq u\\ \frac{1}{N}\left(\left(\frac{N-1}{N}\right)^{N-u-1}+\left(\frac{N-1}{N}\right)^v\right) & v>u\end{cases} \qquad (3.10)$$

za $u,v\in\{0,1,....,(N-1)\}$.
Poredeći (3.9) i (3.10) sledi da je dobijena raspodela neuniformna i da zavisi od reda permutacije $N$. Ovaj rezultat predstavlja polaznu tačku u pokušaju da se odrede raspodele za $S_1,S_2,....$Prvi korak u tom smeru pojavio se u radu [111].

Određivanje raspodele verovatnoća prvog elementa izlaznog niza $z_1$ dat je u sledećoj teoremi.

**Teorema 18** *[111] Pretpostavimo da je inicijalna permutacija $S_0$ za PRGA RC4 izabrana slučajno iz skupa svih mogućih permutacije skupa $\{0,1,2,...,(N-1)\}$. Tada je verovatnoća da je prvi generisani bajt jednak 0 data sa*

$$P\left(z_1=0\right)\approx\frac{1}{N}-\frac{1}{N^2}.$$

**Dokaz.** Primenjujući Bjesovu formulu po $S_0\left[j_1\right]=0$ i $S_0\left[j_1\right]\neq 0$ imamo:

$$\begin{aligned}P\left(z_1=0\right)&=P\left(z_1=0\,|\,S_0\left[j_1\right]=0\right)\cdot P\left(S_0\left[j_1\right]=0\right)\\&+P\left(z_1=0\,|\,S_0\left[j_1\right]\neq 0\right)\cdot P\left(S_0\left[j_1\right]\neq 0\right).\end{aligned} \qquad (3.11)$$

Razmotrimo dva slučaja:
Kada je $S_0\left[j_1\right]=0$

Stavljajući da je

$$j_1 = S_0[1] = X \neq 1$$
$$S_0[j_1] = S_0[S_0[1]] = 0$$

dobijamo

$$z_1 = S_1[S_1[1] + S_1[X]] = S_1[0 + X] = S_0[1] = X \neq 0.$$

što daje

$$P(z_1 = 0 \mid S_0[j_1] = 0) = 0 \tag{3.12}$$

Kada je $S_0[j_1] \neq 0$
Tada možemo smatrati da $z_1$ ima ravnomernu raspodelu

$$P(z_1 = 0 \mid S_0[j_1] \neq 0) \approx 0 \tag{3.13}$$

Zamena (3.12) i (3.13) u (3.11) daje

$$P(Z_1 = 0) \approx 0 \cdot \frac{1}{N} + \frac{1}{N} \cdot \left(1 - \frac{1}{N}\right) = \frac{1}{N} - \frac{1}{N^2}$$

što je i trebalo dokazati. ■

Raspodela kada prvi element izlaznog niza ima vrednost različitu od nule data je sa, [111],

$$P(z_1 = v) = Q_v + \sum_{X \in \mathcal{L}_v} \sum_{Y \in \mathcal{T}_{v,X}} P(S_0[1] = X \wedge S_0[X] = Y \wedge S_0[X + Y] = v)$$

gde je

$$Q_v = \begin{cases} P(S_0[1] = 1 \wedge S_0[2] = 0) & v = 0 \\ P(S_0[1] = 0 \wedge S_0[0] = 1) & v = 1 \\ P(S_0[1] = 1 \wedge S_0[2] = v) + P(S_0[1] = v \wedge S_0[v] = 0) & \\ \quad + P(S_0[1] = 1 - v \wedge S_0[1 - v] = v) & \text{inače} \end{cases}$$

U istom radu pokazano je da je raspodela prvih $z_r$ generisanih bajtova neuniformna tako što je određenja verovatnoća da $P(z_r = 0)$ za $3 \leq r \leq 255$. Ta verovatnoća iznosi

$$P(z_r = 0) = \frac{1}{N} + \frac{c_r}{N^2} \tag{3.14}$$

gde je

$$c_r = \begin{cases} \frac{N}{N-1}(N \cdot P(S_{r-1}[r] = r) - 1) - \frac{N-2}{N-1} & r = 3 \\ \frac{N}{N-1}(N \cdot P(S_{r-1}[r] = r) - 1) & inače \end{cases} \tag{3.15}$$

Na osnovu određene raspodele verovatnoća $P(z_r = 0)$, jednačine (3.14) i (3.15) izvode se sledeće nejednakosti:

$$\frac{1}{N} + \frac{0.242811}{N^2} \leq P(z_r = 0) \leq \frac{1}{N} + \frac{1.337057}{N^2} \tag{3.16}$$

Rad [111] predstavlja iscrpan izvor odstupanja raspodela verovatnoća u pseudoslučajnom generatoru RC4. Do sada navedena a i mnoga druga odstupanja od uniformne raspodele spadaju u kategoriju bliskih odstupanja. Broj i stepen odstupanja od uniformne raspodele predstavlja problem u upotrebi ovog generatora. To je bio prvi indikator bezbednosnih problema sa ovim pseudoslučajnim generatorom. Međutim, smatrajući da su sva odstupanja bliska i da se sa vremenom gube iskristalisalo se mišljenje da je dovoljno rešenje odbaciti izvestan broj početnih bajtova generisanog izlaznog niza a da će se preostali deo ponašati saglasno uniformnoj raspodeli. Kao dovoljna dužina odbačenog dela procenjeno je $6N$. Predloženo rešenje bi bilo zadovoljavajuće pod uslovom da udaljenih odstupanja nema. Na žalost istraživanja su otkrila drugačiju sliku. U radovima [105], [112] [113], [111], prikazana su različita udaljena odstupanja od uniformne raspodele

Prikazaćemo sada jedno daleko odstupanje objavljeno u radu [114].

**Teorema 19** *[114] Nakon r-tog takta PRGA RC4 važi*

$$P(S_r[j_r] = i_r - z_r) \approx \frac{2}{N}$$

**Dokaz.** Posmatrajmo događaje

$$i_r = S_r[i_r] + S_r[j_r]$$

i

$$i_r \neq S_r[i_r] + S_r[j_r]$$

U slučaju kada je $i_r = S_r[i_r] + S_r[j_r]$ imamo

$$\begin{aligned} z_r &= S_r[S_r[i_r] + S_r[j_r]] \\ &= S_r[i_r] = \\ &= i_r - S_r[j_r] \end{aligned}$$

Stavljajući $S_r[j_r] = i_r - z_r$ dobijamo

$$\begin{aligned} &P((S_r[j_r] = i_r - z_r) \wedge (i_r = S_r[i_r] + S_r[j_r])) = \\ &= 1 \cdot \frac{1}{N} = \frac{1}{N} \end{aligned} \tag{3.17}$$

U drugom slučaju događaj $i_r \neq S_r[i_r] + S_r[j_r]$ se realizuje sa verovatnoćom $\frac{(N-1)}{N}$ što znači da se događaj

$$i_r = S_r[i_r] + S_r[j_r]$$

realizuje sa verovatnoćom $\frac{1}{N}$ pa dobijamo

$$\begin{aligned} &P\left((S_r[j_r] = i_r - z_r) \wedge (i_r \neq S_r[i_r] + S_r[j_r])\right) = \\ &= \frac{(N-1)}{N} \cdot \frac{1}{N} = \frac{1}{N} - \frac{1}{N^2} \end{aligned} \tag{3.18}$$

Neka su $D_1$ i $D_2$ sledeći događaji

$$\begin{aligned} D_1 &= \{((S_r[j_r] = i_r - z_r) \wedge (i_r \neq S_r[i_r] + S_r[j_r]))\} \\ D_2 &= \{((S_r[j_r] = i_r - z_r) \wedge (i_r = S_r[i_r] + S_r[j_r]))\}. \end{aligned}$$

Tada je

$$\begin{aligned} \{S_r[j_r] = i_r - z_r\} &= D_1 \cup D_2 \\ D_1 \cap D_2 &= \varnothing \end{aligned}$$

pa sabiranjem verovatnoća (3.17) i (3.18) dobijamo

$$P(S_r[j_r] = i_r - z_r) = \frac{2}{N} - \frac{1}{N^2} \approx \frac{2}{N}$$

što je i trebalo pokazati. ■

Na sličan način se može dokazati i sledeća relacija

$$P(S_r[i_r] = j_r - z_r) \approx \frac{2}{N}.$$

Događaji

$$S_r[j_r] = i_r - z_r$$

i

$$z_r = i_r - S_r[j_r]$$

su ekvivalentni pa je zbog transformacije permutacije u $r-$tom taktu

$$S_r[j_r] = S_{r-1}[r]$$

što daje

$$P(z_r = r - S_{r-1}[r]) \approx \frac{2}{N} \tag{3.19}$$

Relacija data sa (3.19) je efikasno iskorišćena za definisanje kriptoanalizu pseudoslučajnog generatora RC4 u [110].

U [111] je pokazano da su daleka odstupanja imanentna generatoru RC4 pod određenim uslovima, naime važi sledeća relacija:

$$P\left(z_{wN} = 0 \wedge z_{wN+2} = 0\right) = \frac{1}{N^2} + \frac{1}{N^3}.$$

za svako $w \geq 1$.

### 3.2.4 Analiza korelacionih svojstava generatora RC4

Analiza korelacionih svojstava generatora RC4 predstavlja analizu međusobnog uzajamnog uticaja delova pseudoslučajnog generatora a posebno uticaja kriptografskog ključa i delova generatora na izlazni niz. Primena pseudoslučajnog generatora u telekomunikacionim standardima učinila je da postna predmet istraživačkog interesovanja brojnih istraživačkih grupa i pojedinaca. Eksperimentalna i teorijska ispitivanja su ukazala na postojanje brojnih korelacionih relacija u pseudoslučajnom generatoru RC4. Iscrpna lista ovih korelacija se može videti u [111].

Eksperimentalne analize i njihovi rezultati prikazani u [85] su pokazale postojanje značajne korelacije između prvog bajta izlaznog niza $z_1$ i prva tri bajta primenjenog kriptografskog ključa $k_0, k_1, k_3$. Ta eksperimentalna činjenica pokazuje da postoji prelivanje informacija o kriptografskom ključu u izlazni niz i pokazuje kako se praktično može detektovati. Postojanje takve relacije predstavlja ozbiljnu manu za svaki kriptografski algoritam.

Da bi smo pokazali postojanje i utvrdili veličinu te korelacije izračunaćemo verovatnoću

$$P\left(z_1 = k_0 + k_1 + k_2 + 3\right) \tag{3.20}$$

U dokazu ćemo koristiti sledeću lemu.

**Lema 20** $P\left(S_1\left[2\right] = z_1 = k_0 + k_1 + k_2 + 3\right) \approx \left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}$.

**Dokaz.** Dokaz ćemo izvesti uz pretpostavku da promenljiva $j$ ima ravnomernu raspodelu tokom generisanja izlaznog niza iz pseudoslučajnog generatora RC4.
U prvom taktu pseudoslučajnog generatora RC4 vrednost promenljive $i_1$ je 1 a vrednost promenljive $j_1$ je $S_0\left[1\right]$. Odatle sledi da $S_0\left[1\right]$ uvek učestvuje u transformaciji permutacije $S_0$. Druga pozicija koja učestvuje u transformaciji permutacije

$S_0$ zavisi od vrednosti permutacije na poziciji 1, $S_0[1]$.
Neka je sada

$$f(k) = k_0 + k_1 + k_2 + 3. \tag{3.21}$$

Sada koristeći teoremu 14 dobijamo

$$P\left(S_N^0[2] = f(k)\right) \approx \left(\frac{N-1}{N}\right)^N \tag{3.22}$$

Po završetku prvog takta događaj $S_N^0[2] = f(k)$ se može realizovati na dva načina:
**1)** da je događaj nastao u $S_0$ i da pozicija 2 ne učestvuje u transformaciji permutacije $S_0$ u prvom taktu ili,
**2)** u permutaciji $S_0$ je indeks vrednosti $f(k)$ jednak 1 a pri transformaciji permutacije $S_0$ se pozicionira na poziciju sa indeksom 2.
U slučaju da se na kraju KSA procesa desio događaj $S_N^0[2] = f(k)$, a da transformacija permutacije $S_0$ ne učestvuje sadržaj sa pozicije 2 u prvom taktu generisanja izlaznog niza imamo

$$P\left(S_N^0[2] = f(k)\right) \cdot P\left(S_N^0[1] \neq 2\right) = \left(\frac{N-1}{N}\right)^N \cdot \left(1 - \frac{1}{N}\right) \tag{3.23}$$

U slučaju da se na kraju KSA procesa desio događaj $S_N^0[2] \neq f(k)$ i $f(k)$ se pri transformaciji permutacije $S_0$ pojavljuje na poziciji 2 sa pozicije 1 u prvom taktu dobijamo

$$\begin{aligned} &P\left(S_N^0[2] \neq f(k)\right) \cdot P\left(S_N^0[1] = f(k) \wedge S_N^0[1] = 2\right) = \\ &= P\left(S_N^0[2] \neq f(k)\right) \cdot P\left(S_N^0[1] = 2\right) \cdot P\left(f(k) = 2\right) = \\ &= \left(1 - \left(\frac{N-1}{N}\right)^N\right) \cdot \frac{1}{N^2} \end{aligned} \tag{3.24}$$

Sada sabirajući (3.23) i (3.24) imamo

$$P\left(S_N^0[2] = f(k)\right) = \left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2} \tag{3.25}$$

što je i trebalo dokazati. ■

U originalnoj definiciji pseudoslučajnog generatora RC4 je $N = 256$ pa je $P(S_N^0[2] = f(k))$ približno 0.37. Verovatnoća izražena jednačinom (3.25) je verovatnoća $P(S_N^0[1] = 2)$ aproksimirana izrazom $\frac{1}{N}$. Korišćenje tačne vrednosti

$$P\left(S_N^0[1] = 2\right) = \frac{1}{N}\left(\left(\frac{N-1}{N}\right)^{N-2} + \left(\frac{N-1}{N}\right)^2\right)$$

ne utiče značajno na rezultat za velike vrednosti $N$.

Sada smo u poziciji da i teorijski obrazložimo postojanje korelacije između prva tri bajta primenjenog kriptografskog ključa i prvog elementa izlaznog niza.

**Teorema 21** *[102] Za proizvoljno na slučajan način odabran kriptografski ključ $k$ u generatoru RC4 postoji korelacija između prvog generisanog elementa izlaznog niz i prva tri bajta ključa data sa*

$$P\left(z_1 = k_0 + k_1 + k_2 + 3\right) \approx \frac{1}{N} \cdot \left(1 + \left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right).$$

**Dokaz.** Neka je

$$f\left(k\right) = k_0 + k_1 + k_2 + 3.$$

i

$$t_1 = S_1\left[i_1\right] + S_1\left[j_1\right]$$

Prema definiciji pseudoslučajnog generatora za prvi takt važi

$$\begin{aligned}
&P\left(z_1 = f\left(k\right)\right) = \\
&\quad = P\left(S_1\left[t_1\right] = f\left(k\right)\right) = \\
&\quad = \sum_{x=0}^{N-1} P\left(t_1 = x\right) \cdot P\left(S_1\left[t_1\right] = f\left(k\right) \mid t_1 = x\right) = \\
&\quad = \sum_{x=0}^{N-1} P\left(t_1 = x\right) \cdot P\left(S_1\left[x\right] = f\left(k\right)\right) = \\
&\quad = P\left(t_1 = 2\right) \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) + \\
&\qquad\quad + \sum_{\substack{x=0 \\ x \text{ je parno} \neq 2}}^{N-1} P\left(t_1 = x\right) \cdot P\left(S_1\left[x\right] = f\left(k\right)\right) + \\
&\qquad\quad + \sum_{\substack{x=0 \\ x \text{ je neparno}}}^{N-1} P\left(t_1 = x\right) \cdot P\left(S_1\left[x\right] = f\left(k\right)\right) \\
&\quad = \left(\frac{2}{N} - \frac{1}{N\left(N-1\right)}\right) \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) \\
&\qquad\quad + \sum_{\substack{x=0 \\ x \text{ je parno} \neq 2}}^{N-1} \left(\frac{2}{N} - \frac{1}{N\left(N-1\right)}\right) \cdot P\left(S_1\left[x\right] = f\left(k\right)\right)
\end{aligned}$$

$$+ \sum_{\substack{x=0 \\ x \text{ je neparno}}}^{N-1} \frac{1}{N} \cdot P\left(S_1\left[x\right] = f\left(k\right)\right)$$

dalje imamo

$$\begin{aligned}
&P\left(z_1 = f\left(k\right)\right) \approx \\
&\approx \frac{2}{N} \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) + \qquad (3.26) \\
&\qquad + \sum_{\substack{x=0 \\ x \text{ je parno} \neq 2}}^{N-1} \frac{1}{N} \cdot P\left(S_1\left[x\right] = f\left(k\right)\right) \quad \left(\text{jer je } \frac{1}{N\left(N-1\right)} \ll \frac{1}{N}\right) \\
&\qquad + \sum_{\substack{x=0 \\ x \text{ je neparno}}}^{N-1} \frac{1}{N} \cdot P\left(S_1\left[x\right] = f\left(k\right)\right) \qquad (3.27) \\
&= \frac{1}{N} \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) \\
&\qquad + \frac{1}{N} \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) \qquad (3.28) \\
&\qquad + \frac{1}{N} \sum_{\substack{x=0 \\ x \text{ je parno} \neq 2}}^{N-1} P\left(S_1\left[x\right] = f\left(k\right)\right) \\
&\qquad + \frac{1}{N} \sum_{\substack{x=0 \\ x \text{ je neparno}}}^{N-1} P\left(S_1\left[x\right] = f\left(k\right)\right) \\
&= \frac{1}{N} \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) + \frac{1}{N} \cdot \sum_{x=0}^{N-1} P\left(S_1\left[x\right] = f\left(k\right)\right)
\end{aligned}$$

sada koristeći lemu 20 dobijamo

$$\begin{aligned}
P\left(z_1 = f\left(k\right)\right) &\approx \frac{1}{N} \cdot P\left(S_1\left[2\right] = f\left(k\right)\right) + \frac{1}{N} \cdot \sum_{x=0}^{N-1} P\left(S_1\left[x\right] = f\left(k\right)\right) = \\
&= \frac{1}{N} \cdot \left(\left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right) + \frac{1}{N} \cdot 1 = \\
&= \frac{1}{N} \cdot \left(1 + \left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right)
\end{aligned}$$

čime je dokaz završen. ■

Sa statističkog stanovišta poželjno je da promenljive unutrašnjeg stanja i elementi izlaznog niza pseudoslučajnog generatora imaju ravnomernu raspodelu kao i da spregnute verovatnoće raspodela budu ravnomerne.

U terminima oznaka uvedenih u teoremi 21, to bi značilo da spregnuta slučajna promenljiva $(z_1, f(k))$ ima ravnomernu raspodelu odnosno:

$$P(z_1 = f(k)) = \sum_{x=0}^{N-1} P(z_1 = x, f(k) = x) = \\ = \sum_{x=0}^{N-1} \frac{1}{N^2} = N \cdot \frac{1}{N^2} = \frac{1}{N}$$

što je negirano Teoremom 21. Kada je $N = 256$ vrednost koju daje Teorema 21 je 0.0039 dok je eksperimentalno dobijena vrednost bitno veća 0.0053.

Rezultati nekih eksperimenata indiciraju da postojeće odstupanje $z_1$ od ravnomerne raspodela nije posledica prirode promenljive $z_1$ već ukazuju na prelivanje neuniformnosti u raspodeli slučajne promenljive $t_1$ na $z_1$.

Sledeća teorema demonstrira mehanizam prelivanja neravnomernosti u raspodeli.

**Teorema 22** *[84] Ako je u generatoru RC4 odabran ključ $k$ tako da je $k_0 + k_1 = 0$ tada za $S_1[i_1] + S_1[j_1]$ važi*

$$P(S_1[i_1] + S_1[j_1] = 2 \,|\, k_0 + k_1 = 0) > \left(\frac{N-1}{N}\right)^N$$

**Dokaz.** Dokaz je pravolinijski.

$$\begin{aligned}
&P(S_1[i_1] + S_1[j_1] = 2 \,|\, k_0 + k_1 = 0) \\
&= P(S_1[i_1] = 1, S_1[j_1] = 1 \,|\, k_0 + k_1 = 0) + \\
&+ \sum_{\substack{x=0 \\ x \neq 1, \frac{N+2}{2}}}^{N-1} P(S_1[i_1] = x, S_1[j_1] = N - x + 2 \,|\, k_0 + k_1 = 0) \\
&> P(S_1[i_1] = 1, S_1[j_1] = 1 \,|\, k_0 + k_1 = 0) \\
&= P(S_1[1] = 1 \,|\, k_0 + k_1 = 0) \\
&(\text{jer je } (S_1[i_1] = 1 \wedge S_1[j_1] = 1) \Longleftrightarrow S_1[1] = 1) \\
&= P(S_1[1] = k_0 + k_1 + 1 \,|\, k_0 + k_1 = 0) \approx \\
&\approx P(S_1[1] = k_0 + k_1 + 1) \\
&\approx \left(\frac{N-1}{N}\right)^N \qquad (\text{zbog Teoreme 14})
\end{aligned}$$

■

Eksperimentalnom analizom u [85] je dobijeno da kada za primenjeni kriptografski ključ važi $k_0 + k_1 = 0$ tada je verovatnoća da je $z_1 = k_2 + 3$ između 0.12 i 0.16.

Teorijska potvrda postojanja korelacije između događaja $k_0+k_1 = 0$ i $z_1 = k_2+3$ data je sledećom teoremom.

**Teorema 23** *[102] Ako je u generatoru RC4 odabran ključ k tako da je* $k_0+k_1 = 0$ *tada postoji korelacija između bajtova ključa i prvog izlaznog bajta data sa*

$$P\left(z_1 = k_2 + 3 \,|\, k_0 + k_1 = 0\right) > \left(\frac{N-1}{N}\right)^N \cdot \left(\left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right)$$

**Dokaz.** Neka je $t_1 = S_1\left[i_1\right] + S_1\left[j_1\right]$ tada imamo

$$\begin{aligned}
&P\left(z_1 = k_2 + 3 \,|\, k_0 + k_1 = 0\right) \\
&= P\left(S_1\left[t_1\right] = k_2 + 3 \,|\, k_0 + k_1 = 0\right) \\
&= \sum_{x=0}^{N-1} P\left(t_1 = x \,|\, k_0 + k_1 = 0\right) \cdot P\left(S_1\left[t_1\right] = k_2 + 3 \,|\, k_0 + k_1 = 0, t_1 = x\right) \\
&= \sum_{x=0}^{N-1} P\left(t_1 = x \,|\, k_0 + k_1 = 0\right) \cdot P\left(S_1\left[x\right] = k_2 + 3 \,|\, k_0 + k_1 = 0\right) \\
&> P\left(t_1 = 2 \,|\, k_0 + k_1 = 0\right) \cdot P\left(S_1\left[2\right] = k_2 + 3 \,|\, k_0 + k_1 = 0\right) \\
&= P\left(t_1 = 2 \,|\, k_0 + k_1 = 0\right) \cdot P\left(S_1\left[2\right] = k_0 + k_1 + k_2 + 3 \,|\, k_0 + k_1 = 0\right) \approx \\
&\approx P\left(t_1 = 2 \,|\, k_0 + k_1 = 0\right) \cdot P\left(S_1\left[2\right] = k_0 + k_1 + k_2 + 3 \,|\, k_0 + k_1 = 0\right) \\
&\approx \left(\frac{N-1}{N}\right)^N \cdot \left(\left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right)
\end{aligned}$$

čime je dokaz završen. ■

Kada je $N = 256$ numerička vrednost izraza $\left(\frac{N-1}{N}\right)^N \cdot \left(\left(\frac{N-1}{N}\right)^N \left(1 - \frac{1}{N} - \frac{1}{N^2}\right) + \frac{1}{N^2}\right)$ je 0.13 što odgovara registrovanim eksperimentalnim vrednostima.

# Glava 4

# Klasa pouzdanih kriptografskih pseudoslučajnih generatora

Postizanje visokog nivoa informacione bezbednosti predstavlja imperativ u današnjem digitalizovanom društvu. Osnova svih bezbednosnih rešenja su različite kriptografske metode i algoritmi. Svako od tih rešenja predstavlja složen mehanizam u kojem propust u bilo kom delu može ruinirati ceo sistem, [120] [121]. Zbog toga je sinteza kriptoloških algoritama kompleksan i odgovoran zadatak. Situacija se dodatno usložnjava kada kriptografske algoritme treba primeniti u okruženjima sa ograničenim računarskim resursima kao što su bežične senzorske mreže (WSN) ili Internet stvari (IoT). U računarski ograničenim okruženjima se uobičajeno primenjuju sekvencijalni kriptografski algoritmi zbog ostvarivog visokog nivoa bezbednosti te kompaktnosti i efikasnosti implementacije bilo u hardveru bilo u softveru. Sekvencijalni kriptografski algoritmi se uobičajeno realizuju kao aditivni pseudoslučajni generatori i stoga se sinteza kvalitetnih kriptografskih algoritama tog tipa svodi na sintezu kvalitetnih pseudoslučajnih generatora. Motivacija za ovaj rad je bila višestruka.

Prvi izazov koji se javlja u ovom kontekstu je sinteza pouzdanog pseudoslučajnog generatora za računarski ograničena okruženja.

Drugi izazov je željena struktura pseudoslučajnog generatora. Ideja vodilja je bila da se kreira parametrizovan pseudoslučajni generator, klasa pseudoslučajnih generatora, ali tako da:

1. Skup mogućih vrednosti parametara bude brojan, tako da se mogu kreirati i koristiti brojni konkretni pseudoslučajni generatori koji pri izboru različitih

parametara neće biti međusobno korelisani.

2. Bezbednosne karakteristike definisane klase zavise samo od pripadnosti parametara željenom skupu parametara a ne od konkretnih vrednosti parametara.

Treći izazov je bila upotreba promenljivih permutacija koja je kroz RC4 generator i njemu srodne modifikacije potpuno odbačena [100].

Istraživanje vođeno prethodno nabrojanim ciljevima rezultiralo je kreiranjem modela odgovarajućeg slučajnog procesa koji je poslužio za definisanje željenog pseudoslučajnog generatora.

## 4.1 Matematički model referentnog slučajnog procesa

Neka je dat skup $I_k = \{0, 1, \ldots, k-1\}$ i skup svih njegovih permutacija $\mathcal{P}_k$. Neka je dalje dat skup $S = \{f_0, f_1, \ldots, f_{m-1}\} \subseteq \mathcal{P}_k$ takav da permutacije $f_i$, $i = 0, 1, ..., (m-1)$ zadovoljavaju sledeće uslove:

1. Neka je $\Pi_j \in \mathcal{P}_k$, $j = 1, 2, \ldots, k!$,proizvoljna permutacija tada postoji ceo broj $l > 0$ i niz prirodnih brojeva $i_1, i_2, \ldots, i_l \in I_m$ tako da je

$$\Pi_j = f_{i_1} \circ \ldots \circ f_{i_{l-1}} \circ f_{i_l},$$

   gde $\circ$ predstavlja operaciju kompozicije funkcija. Drugim rečima $\langle S \rangle = \mathcal{P}_k$.

2. Za proizvoljne cele brojeve $p, q \in I_m$ važi

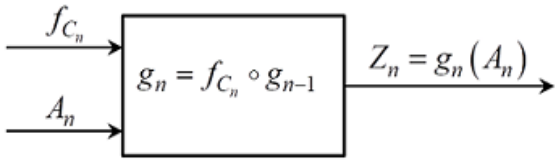
$$(p \neq q) \Longrightarrow (f_p \neq f_q)\,. \tag{4.1}$$

3. Identična permutacija skupa $I_k$,u oznaci, $I$, pripada skupu $S$, $\Pi_1 = I \in S$.

Neka su $A, C$ dve nezavisne slučajne promenljive koje uzimaju vrednosti iz $I_k$ i $I_m$ sa funkcijama raspodele $P\{A = l\} = a_l, \quad l = 0, 1, ..., k-1$ i $P\{C = l\} = c_l, \quad l = 0, 1, ..., (m-1)$ respektivno.

Neka su dalje data dva slučajna procesa $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$ kao realizacije nezavisnih slučajnih promenljivih $A$ i $C$ u vremenu.

Definišimo sada slučajni proces $\{Z_n\}_{n=1}^{\infty}$ gde $Z_n \in I_k$.




Slika 4.1: Grafički prikaz računanja vrednosti $Z_n$

**Definicija 24** ***(RSP)*** *Neka su data dva slučajna procesa $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$ kao realizacije nezavisnih slučajnih promenljivih $A$ i $C$ u vremenu. Slučajni proces $\{Z_n\}_{n=1}^{\infty}$ gde $Z_n \in I_k$ dat je sledećim sistemom jednačina:*

$$\begin{aligned} g_0 &= p & p &\in \mathcal{P}_k \\ g_{n+1} &= f_{C_{n+1}} \circ g_n & n &\geq 0 \\ Z_{n+1} &= g_{n+1}(A_{n+1}) & n &\geq 0. \end{aligned} \tag{4.2}$$

Na osnovu sistema jednačina (4.2) je jasno kako u $n-$tom trenutku slučajna promenljiva $Z_n$ dobija vrednost. Na osnovu vrednosti slučajne promenljive $C_n$ iz skupa $S$ se uzima permutacija $f_{C_n}$ i formira permutacija $g_n = f_{C_n} \circ g_{n-1}$ a potom izračuna vrednost permutacije $g_n$ u tački $A_n$, $Z_n = g_n(A_n)$. Grafički prikaz određivanja vrednosti slučajnog procesa $\{Z_n\}_{n=1}^{\infty}$ je dat na slici 4.1

Slučajni proces $\{Z_n\}_{n=1}^{\infty}$ se odvija tako što se u svakom taktu, koristeći slučajni proces $\{C_n\}_{n=1}^{\infty}$ menja permutacija $g_n$ iz koje se dobija vrednost $Z_n$ na osnovu vrednosti slučajnog procesa $\{A_n\}_{n=1}^{\infty}$. Vrednosti $\{Z_n\}_{n=1}^{\infty}$ ćemo zvati izlaznim nizom opisanog slučajnog procesa.

### 4.1.1 Analiza osobina slučajnog procesa $\{Z_n\}_{n=1}^{\infty}$

Za svaki slučajni proces neophodno je analizirati njegove statističke osobine u smislu funkcije raspodele vrednosti izlaznog niza i njegove prediktabilnosti. U tom smislu poželjne osobine su ravnomerna raspodela za vrednosti izlaznog niza, neprediktabilnost vrednosti izlaznog niza, neznatna količina informacija koju izlazni niz nosi o slučajnom procesu i druge.

#### 4.1.1.1 Funkcija raspodele verovatnoća $\{Z_n\}_{n=1}^{\infty}$

Prirodno bi bilo očekivati, s obzirom na način formiranja $Z_n$ i činjenicu da je $\langle S \rangle = \mathcal{P}_k$, da $\{Z_n\}_{n=1}^{\infty}$ ima uniformnu raspodelu izlaznih vrednost ali je takođe

jasno da to mora zavisiti i od raspodela za $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$. Sledeća teorema definiše dovoljne uslove pod kojima $\{Z_n\}_{n=1}^{\infty}$ ima asimptotski uniformnu raspodelu.

**Teorema 25** *[115] Ako $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$ ispunjavaju sledeće uslove*

1. $\sum_{i=1}^{k} a_i = 1$ *i* $a_i > 0$ *za sve* $i \in I_k$,

2. $\sum_{i=0}^{m-1} c_i = 1$ *i* $c_i > 0$ *za sve* $i \in I_m$,

*tada izlazni niz slučajnog procesa $\{Z_n\}_{n=1}^{\infty}$ima asimptotski uniformnu raspodelu datu sa*

$$(\forall l \in I_k) \quad \left( \lim_{n\to\infty} P\{Z_n = l\} = \frac{1}{k} \right)$$

*za sve $l \in I_k$.*

Dokaz Teoreme 25 izvodi se u dva koraka. U prvom koraku koristeći teoriju Markovljevih lanaca se pokazuje da niz permutacija $\{g_n\}_{n=0}^{\infty}$ ima asimptotski uniformnu raspodelu a potom, u drugom koraku, koristeći tu činjenicu dokazaćemo tvrđenje Teoreme 25.

**Dokaz.** Kao što je rečeno, prvo ćemo posmatrati niz permutacija $\{g_n\}_{n=0}^{\infty}$.
Kako je $(\mathcal{P}_k, \circ)$ grupa i s obzirom na način dobijanja $g_n$ dat u (4.2) sledi da je $g_n$ permutacija odnosno $g_n \in \mathcal{P}_k$.Dokažimo sada da niz permutacija $\{g_n\}_{n=0}^{\infty}$ ima asimptotski uniformnu raspodelu odnosno da je

$$(\forall i \in \{1, 2, \ldots, k!\}) \left( \lim_{n\to\infty} P\{g_n = \Pi_i\} = \frac{1}{k!} \right). \tag{4.3}$$

Da bi smo dokazali (4.3) posmatraćemo niz $\{g_n\}_{n=0}^{\infty}$ kao stacionaran Markovljev lanac nad skupom stanja $\mathcal{P}_k$.
Zaista, u skladu sa definicijom niza $\{g_n\}_{n=0}^{\infty}$datom u (4.2) prelazak iz stanja $g_n$ u $g_{n+1}$ zavisi jedino od tekućeg stanja $g_n$ i vrednosti $A_n$ ali ne i od istorije procesa $\{g_n\}_{n=0}^{\infty}$.
Označimo sa $G_n = [P\{g_n = \Pi_i\}]_{1\times k!}$ matricu vrstu čiji su elementi verovatnoće da se posle $n$ koraka posmatrani Markovljev lanac nađe u stanju $\Pi_i$. Neka je $T = [t_{i\,j}]_{k!\times k!}$ matrica prelaska ovog Markovljevog procesa u jednom koraku a $t_{i\,j}$ verovatnoća da Markovljev proces iz stanja $\Pi_i$ pređe u stanje $\Pi_j$ u jednom koraku. Primetimo da je $T = [t_{i\,j}]_{k!\times k!}$ bistohastička matrica.
Slično sa $T_n = \left[t_{i\,j}^{n}\right]_{k!\times k!}$ označimo matricu prelaska Markovljevog procesa u $n$

koraka gde $t_{ij}^n$ označava verovatnoću da lanac iz stanja $\Pi_i$ pređe u stanje $\Pi_j$ u $n$ koraka. Poznato je da je $T_n = T^n$ i matrica $T_n = \left[t_{ij}^n\right]_{k!\times k!}$ je takođe bistohastička, [117] [118]. U skladu sa uvedenim oznakama imamo da je

$$\begin{aligned} G_n &= G_0 T_n \\ \lim_{n\to\infty} G_n &= \lim_{n\to\infty} G_0 T_n = G_0 \lim_{n\to\infty} T_n \end{aligned} \tag{4.4}$$

kada granične vrednosti u (4.4) postoje. Dovoljan uslov za postojanje granične vrednosti $\lim\limits_{n\to\infty} T_n$ je da postoji prirodan broj $n_0 \in \mathbb{N}$ tako da je $t_{ij}^{n_0} > 0$ za sve $i, j \in \{1, 2, ..., k!\}$, [117], [118].
Da bi smo utvrdili postojanje takvog broja $n_0$ definišimo brojeve $n_{ij}$ na sledeći način

$$n_{ij} = \min_r \left\{ r \mid (\exists (i_1, i_2, \ldots, i_r) \in I_m) \left( f_{i_1} \circ \ldots \circ f_{i_{r-1}} \circ f_{i_r} = \Pi_j \circ \Pi_i^{-1} \right) \right\}. \tag{4.5}$$

Imajući u vidu da je $\langle S \rangle = \mathcal{P}_k$, uslov 1. u (4.1) imamo da je $n_{ij} > 0$. Stavimo

$$n_0 = \max_{i,j\in\{1,2,\ldots,k!\}} n_{ij}$$

Pokažimo sada da je $t_{ij}^{n_0} > 0$ za sve $i, j \in \{1, 2, ..., k!\}$.
Pošto je $(\mathcal{P}_k, \circ)$ grupa tada jednačina $x \circ \Pi_i = \Pi_j$ ima tačno jedno rešenje dato sa $x = \Pi_j \circ \Pi_i^{-1}$ imamo

$$\begin{aligned} t_{ij}^{n_0} &= \sum_{(i_1,\ldots,i_{n_0})} P\left\{ f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_{n_0}} \circ \Pi_i = \Pi_j \right\} \\ &= \sum_{(i_1,\ldots,i_{n_0})} P\left\{ f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_{n_0}} = \Pi_j \circ \Pi_i^{-1} \right\} \\ &= \sum_{\substack{(i_1,\ldots,i_{n_0}) \\ f_{i_1}\circ f_{i_2}\circ\ldots\circ f_{i_{n_0}} = \Pi_i^{-1}\circ\Pi_j}} \prod_{l=1}^{n_0} P\left\{C_l = i_l\right\} \end{aligned} \tag{4.6}$$

Da bi smo pokaza li da je $t_{ij}^{n_0} > 0$ dovoljno je pokazati da je barem jedan sabirak u (4.6) veći od nule, [117] [118]. Pošto je $n_0 \geq n_{ij} > 0$ tada postoji niz prirodnih brojeva $\left\{i_1, i_2, \ldots, i_{n_{ij}}\right\}$, $n_{ij} \leq n_0$ tako da je $f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_{n_{ij}}} = \Pi_i^{-1} \circ \Pi_j$ . Kako je indeks jedinične permutacije 1 sabirak koji odgovara nizu prirodnih brojeva $\left\{ i_1, i_2, \ldots, i_{n_{ij}}, \underbrace{1, 1, \ldots, 1}_{n_0 - n_{ij} \geq 0} \right\}$ je očigledno veći od nule i time smo pokazali da $\lim\limits_{n\to\infty} T_n$

postoji. Prema tome i svaka granična vrednost $\lim_{n\to\infty} t_{ij}^n = t_j^*$ postoji. Granična vrednost $\lim_{n\to\infty} T_n$ se određuje kao rešenje sistema jednačina Čempmen-Kolmogorova

$$\begin{aligned} \sum_{j=1}^{k!} t_j^* t_{jl} &= t_l^* \\ \sum_{j=1}^{k!} t_j^* &= 1 \end{aligned} \tag{4.7}$$

Lako se vidi, zamenom u sistem( 4.7), da je jedno rešenje $t_1^* = t_2^* = \ldots = t_{k!}^* = \frac{1}{k!}$ a jedinstvenost sledi iz jedinstvenosti granične vrednosti.
Dokaz je dalje pravolinijski.
Neka je $l \in I_k$ proizvoljno, tada

$$\begin{aligned} P\{Z_n = l\} &= P\{g_n(A_n) = l\} \\ &= \sum_{i=1}^{k!} P\{g_n(A_n) = l \mid g_n = \Pi_i\}\ P\{g_n = \Pi_i\} \\ &= \sum_{i=1}^{k!} P\{\Pi_i(A_n) = l \mid g_n = \Pi_i\}\ P\{g_n = \Pi_i\} \\ &= \sum_{i=1}^{k!}\sum_{j=0}^{k-1} P\{\Pi_i(j) = l \mid A_n = j\}\ P\{A_n = j\}\, P\{g_n = \Pi_i\}. \end{aligned} \tag{4.8}$$

Kako su $\{\Pi_i(j) = l\}$ i $\{A_n = j\}$ nezavisne slučajne promenljive iz (4.8) sledi da je

$$\begin{aligned} P\{Z_n = l\} &= \sum_{i=1}^{k!}\sum_{j=0}^{k-1} P\{\Pi_i(j) = l \mid A_n = j\}\ P\{A_n = j\}\, P\{g_n = \Pi_i\} \\ &= \sum_{i=1}^{k!}\sum_{j=0}^{k-1} P\{\Pi_i(j) = l\}\ P\{A_n = j\}\, P\{g_n = \Pi_i\} \\ &= \sum_{j=0}^{k-1} P\{A_n = j\} \sum_{i=1}^{k!} P\{g_n = \Pi_i\}\, P\{\Pi_i(j) = l\} \end{aligned} \tag{4.9}$$

Primenjujući graničnu vrednost na levu i desnu stranu jednakosti (4.9) dobijamo

$$\begin{aligned} \lim_{n\to\infty} P\{Z_n = l\} &= \lim_{n\to\infty} \sum_{j=0}^{k-1} P\{A_n = j\} \sum_{i=1}^{k!} P\{g_n = \Pi_i\}\, P\{\Pi_i(j) = l\} \\ &= \sum_{j=0}^{k-1} P\{A_n = j\} \sum_{i=1}^{k!} P\{\Pi_i(j) = l\} \lim_{n\to\infty} P\{g_n = \Pi_i\} \end{aligned} \tag{4.10}$$

jer $P\{A_n = j\}$, $P\{\Pi_i(j) = l\}$ ne zavise od $n$. Koristeći $\lim_{n\to\infty} \mathrm{P}\{g_n = \Pi_i\} = \frac{1}{k!}$ iz (4.10) i zamenjujući u (4.10) dobijamo

$$\begin{aligned}
\lim_{n\to\infty} P\{Z_n = l\} &= \sum_{j=0}^{k-1} P\{A_n = j\} \sum_{i=1}^{k!} P\{\Pi_i(j) = l\} \lim_{n\to\infty} P\{g_n = \Pi_i\} \\
&= \frac{1}{k!} \sum_{j=0}^{k-1} P\{A_n = j\} \sum_{i=1}^{k!} P\{\Pi_i(j) = l\} \\
&= \frac{1}{k!} \sum_{j=0}^{k-1} P\{A_n = j\} (k-1)! \\
&= \frac{(k-1)!}{k!} \sum_{j=0}^{k-1} P\{A_n = j\} \\
&= \frac{1}{k}
\end{aligned}$$

čime je dokaz teoreme završen. ■

**Remark 26** *[115] Asimptotski uniformna raspodela za slučajnu promenljivu $Z_n$, je kao što smo videli u dokazu Teoreme 25 posledica asimptotski uniformne raspodele za permutaciju $g_n$. Kada bi raspodela verovatnoća permutacija početnog stanja bila uniformna $G_0 = \left[\frac{1}{k!}, \frac{1}{k!}, \ldots, \frac{1}{k!\,i}\right]_{1\times k!}$ lako se vidi da i $g_n$ ima uniformnu raspodelu. Kao i u Teoremi 25 ta se raspodela prenosi i na slučajne promenljive $Z_n$, $n = 1, 2, \ldots$ koje onda takođe imaju uniformnu raspodelu.*

**Teorema 27** *[115] Ako slučajne promenljive $A_n$, $n = 1, 2, \ldots\ldots$ imaju uniformnu raspodelu tada za svako $z \in I_k$*

$$P\{Z_n = z\} = \frac{1}{k}$$

**Dokaz.** Po definiciji (4.2) imamo

$$\begin{aligned}
P\{Z_n = z\} &= \sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\{Z_n = z \,|\, g_n = \Pi_i \wedge A_n = j\} \cdot P\{\, g_n = \Pi_i \wedge A_n = j\} \\
&= \sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\{\Pi_i(j) = z\} \cdot P\{\, g_n = \Pi_i\} \cdot P\{A_n = j\} \qquad (4.11)
\end{aligned}$$

zbog nezavisnosti slučajnih promenljivih. Kako $A_n$ ima uniformnu raspodelu iz (4.11) sledi da je

$$\begin{aligned} P\{Z_n = z\} &= \sum_{i=1}^{k!}\sum_{j=0}^{k-1} P\{\Pi_i(j) = z\} \cdot P\{g_n = \Pi_i\} \cdot \frac{1}{k} \\ &= \frac{1}{k}\sum_{i=1}^{k!}\sum_{j=0}^{k-1} P\{\Pi_i(j) = z\} \cdot P\{g_n = \Pi_i\} \\ &= \frac{1}{k}\sum_{i=1}^{k!} P\{g_n = \Pi_i\} \sum_{j=0}^{k-1} P\{\Pi_i(j) = z\} \\ &= \frac{1}{k} \end{aligned}$$

jer je $\sum_{i=1}^{k!} P\{g_n = \Pi_i\} = 1$ i $\sum_{j=0}^{k-1} P\{\Pi_i(j) = z\} = 1$.
Ovim je teorema dokazana. ■

#### 4.1.1.2 Korelacione osobine slučajnog procesa $\{Z_n\}_{n=1}^{\infty}$

**Teorema 28** *[115] Ako slučajne promenljive $A_n$, $n = 1, 2, \ldots\ldots$ imaju uniformnu raspodelu tada za svako $a, b$ takvo da $a, b \in I_k$, važi:*

1. $P\{Z_{n+l} = b \wedge Z_n = a\} = \frac{1}{k^2}$,

2. $P\{Z_{n+l} = b \,|\, Z_n = a\} = \frac{1}{k}$.

**Dokaz.**

1. Primenjujući definiciju slučajnog procesa $\{Z_n\}_{n=1}^{\infty}$ dobijamo

$$\begin{aligned} &P\{Z_{n+l} = b \wedge Z_n = a\} = P\{g_{n+k}(A_{n+k}) = b \wedge g_n(A_n) = a\} = \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\{g_{n+k}(A_{n+k}) = b \wedge g_n(A_n) = a \,|\, g_{n+k} = \Pi_i \wedge g_n = \Pi_j\} \\ &\qquad\qquad \cdot P\{g_{n+k} = \Pi_i \wedge g_n = \Pi_j\} \quad (4.12) \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\{\Pi_i(A_{n+k}) = b \wedge \Pi_j(A_n) = a\} \cdot P\{g_{n+k} = \Pi_i \wedge g_n = \Pi_j\} \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\{\Pi_i(A_{n+k}) = b \wedge \Pi_j(A_n) = a\} \cdot P\{g_{n+k} = \Pi_i \,|\, g_n = \Pi_j\} \end{aligned}$$

$$\cdot P\left\{g_n = \Pi_j\right\}.$$

Koristeći oznake iz Teoreme 25,

$$t_{i,j}^k = P\left\{g_{n+k} = \Pi_i \,|\, g_n = \Pi_j\right\} \tag{4.13}$$

i stavljajući u (4.12) sledi da je

$$\begin{aligned} &P\left\{Z_{n+l} = b \wedge Z_n = a\right\} = \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{\Pi_i\left(A_{n+k}\right) = b \wedge \Pi_j\left(A_n\right) = a\right\} \cdot P\left\{g_{n+k} = \Pi_i \,|\, g_n = \Pi_j\right\} \\ &\qquad\qquad \cdot P\left\{g_n = \Pi_j\right\} \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{\Pi_i\left(A_{n+k}\right) = b \wedge \Pi_j\left(A_n\right) = a\right\} \cdot t_{i,j}^k \cdot P\left\{g_n = \Pi_j\right\}. \end{aligned} \tag{4.14}$$

Pošto su $\Pi_i, \Pi_j$ permutacije onda je

$$P\left\{\Pi_i\left(A_{n+k}\right) = b \wedge \Pi_j\left(A_n\right) = a\right\} = P\left\{A_{n+k} = \Pi_i^{-1}\left(b\right) \wedge A_n = \Pi_j^{-1}\left(a\right)\right\}. \tag{4.15}$$

Koristeći činjenicu da su $A_{n+k}$ i $A_n$ nezavisne slučajne promenljive iz (4.14) i (4.15) sledi da je

$$\begin{aligned} &P\left\{Z_{n+l} = b \wedge Z_n = a\right\} = \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{\Pi_i\left(A_{n+k}\right) = b \wedge \Pi_j\left(A_n\right) = a\right\} \cdot t_{i,j}^k \cdot P\left\{g_n = \Pi_j\right\} \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{A_{n+k} = \Pi_i^{-1}\left(b\right) \wedge A_n = \Pi_j^{-1}\left(a\right)\right\} \cdot t_{i,j}^k \cdot P\left\{g_n = \Pi_j\right\} \\ &= \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{A_{n+k} = \Pi_i^{-1}\left(b\right)\right\} \cdot P\left\{A_n = \Pi_j^{-1}\left(a\right)\right\} \cdot t_{i,j}^k \cdot P\left\{g_n = \Pi_j\right\}. \end{aligned} \tag{4.16}$$

Koristeći pretpostavku da $A_{n+k}$ i $A_n$ imaju uniformnu raspodelu iz (4.16) dobijamo

$$\begin{aligned} &P\left\{Z_{n+l} = b \wedge Z_n = a\right\} = \\ &\quad = \sum_{i=1}^{k!}\sum_{j=1}^{k!} P\left\{A_{n+k} = \Pi_i^{-1}\left(b\right)\right\} \cdot P\left\{A_n = \Pi_j^{-1}\left(a\right)\right\} \cdot t_{i,j}^k \cdot P\left\{g_n = \Pi_j\right\} \end{aligned}$$

$$= \sum_{i=1}^{k!} \sum_{j=1}^{k!} \frac{1}{k} \cdot \frac{1}{k} \cdot t_{i,j}^{k} \cdot P\{g_n = \Pi_j\} \tag{4.17}$$
$$= \frac{1}{k^2} \sum_{i=1}^{k!} P\{g_n = \Pi_i\} \sum_{j=1}^{k!} t_{i,j}^{k}$$
$$= \frac{1}{k^2}$$

jer je $\sum_{j=1}^{k!} t_{i,j}^{k} = 1$ i $\sum_{i=1}^{k!} P\{g_n = \Pi_i\} = 1$, čime je tvrđenje dokazano.

2. Koristeći tvrđenje Teoreme 27 da je $P\{Z_n = a\} = \frac{1}{k}$ i definiciju uslovne verovatnoće imamo

$$P\{Z_{n+l} = b \,|\, Z_n = a\} = \frac{P\{Z_{n+k} = b \wedge Z_n = a\}}{P\{Z_n = a\}} = \frac{\frac{1}{k^2}}{\frac{1}{k}} = \frac{1}{k}$$

što dokazuje tvrđenje 2.

■

#### 4.1.1.3 Prelivanje informacija u slučajnom procesu $\{Z_n\}_{n=1}^{\infty}$

Pod prelivanjem informacija u slučajnom procesu $\{Z_n\}_{n=1}^{\infty}$ podrazumeva se količina informacija koju slučajna promenljiva $Z_n$ nosi o slučajnim promenljivim $A_n$ i $C_n$. U suštini to je utvrđivanje postojanja zavisnosti između izlaznog niza i elemenata unutrašnjeg stanja slučajnog procesa kao i njeno kvantifikovanje u slučaju postojanja. U ovom odeljku se razmatra postojanje zavisnosti između slučajnih promenljivih $A_n$, $C_n$ i $Z_n$.

**Teorema 29** *[115] Ako važe uslovi Teoreme 25 tada važi*

1. $\lim_{n\to\infty} P(Z_n = z \,|\, C_n = c) = \frac{1}{k}$
2. $\lim_{n\to\infty} I(Z_n, C_n) = 0$

pri čemu $z \in I_k$ i $c \in I_m$

**Dokaz.**

1. Po definiciji uslovne verovatnoće imamo

$$\begin{aligned} &P\left(Z_n = z \,|\, C_n = c\right) = \\ &= \frac{P\left(Z_n = z \wedge C_n = c\right)}{P\left(C_n = c\right)} = \frac{P\left(g_n\left(A_n\right) = z \wedge C_n = c\right)}{P\left(C_n = c\right)} \\ &= \frac{P\left(\left(\bigcup_{i=1}^{k!} g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)}{P\left(C_n = c\right)} \\ &= \frac{P\left(\left(\bigcup_{i=1}^{k!} f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)}{P\left(C_n = c\right)} \\ &= \frac{P\left(\bigcup_{i=1}^{k!} \left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)\right)}{P\left(C_n = c\right)}. \end{aligned} \tag{4.18}$$

Kako su $\{f_{C_n} \circ g_{n-1} = \Pi_i\}$ i $\{f_{C_n} \circ g_{n-1} = \Pi_j\}$ disjunktni događaji to za $i, j \in I_k$ i $i \neq j$ iz jednakosti (4.18) sledi da je

$$\begin{aligned} P\left(Z_n = z | C_n = c\right) &= \frac{P\left(\bigcup_{i=1}^{k!} \left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)\right)}{P\left(C_n = c\right)} \\ &= \frac{\sum_{i=1}^{k!} P\left(\left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)\right)}{P\left(C_n = c\right)} \end{aligned} \tag{4.19}$$

Koristeći Bajesovu teoremu iz jednakosti (4.19) sledi

$$\begin{aligned} P\left(Z_n = z \,|\, C_n = c\right) &= \frac{\sum_{i=1}^{k!} P\left(\left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right)\right)}{P\left(C_n = c\right)} \\ &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(\left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge C_n = c\right) | \left(A_n = j\right)\right) \cdot P\left(A_n = j\right)}{P\left(C_n = c\right)} \end{aligned} \tag{4.20}$$

$$\begin{aligned} &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(\left(\left(f_{C_n} \circ g_{n-1} = \Pi_i \wedge \Pi_i\left(j\right) = z\right) \wedge C_n = c\right)\right) \cdot P\left(A_n = j\right)}{P\left(C_n = c\right)} \\ &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right) \wedge \Pi_i\left(j\right) = z\right) \cdot P\left(A_n = j\right)}{P\left(C_n = c\right)}. \end{aligned}$$

Pošto su događaji $\left\{g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right\}$ i $\{\Pi_i(j) = z\}$ nezavisni iz (4.20) sledi

$$\begin{aligned} &P(Z_n = z \,|\, C_n = c) = \\ &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right) \wedge \Pi_i(j) = z\right) \cdot P(A_n = j)}{P(C_n = c)} \\ &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right) \cdot P(\Pi_i(j) = z) \cdot P(A_n = j)}{P(C_n = c)} \end{aligned} \tag{4.21}$$

Menjajući redosled sabiranja u (4.21) grupisanjem sabiraka koji zavise od $j$ dobijamo

$$\begin{aligned} &P\ (Z_n = z \,|\, C_n = c) = \\ &= \frac{\sum_{i=1}^{k!} \sum_{j=0}^{k-1} P\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right) \cdot P(\Pi_i(j) = z) \cdot P(A_n = j)}{P(C_n = c)} \\ &= \sum_{i=1}^{k!} \frac{P\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right) \sum_{j=0}^{k-1} P(A_n = j) \cdot P(\Pi_i(j) = z)}{P(C_n = c)} \\ &= \sum_{i=1}^{k!} \frac{P\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i \wedge C_n = c\right)}{P(C_n = c)} \sum_{j=0}^{k-1} P(A_n = j) \cdot P(\Pi_i(j) = z) \\ &= \sum_{i=1}^{k!} P\left(g_{n-1} = f_{C_n}^{-1} \circ \Pi_i | C_n = c\right) \sum_{j=0}^{k-1} P(A_n = j) \cdot P(\Pi_i(j) = z) \\ &= \sum_{i=1}^{k!} P\left(g_{n-1} = f_c^{-1} \circ \Pi_i\right) \sum_{j=0}^{k-1} P(A_n = j) \cdot P(\Pi_i(j) = z) \end{aligned} \tag{4.22}$$

Prelazeći na granični proces na obe strane jednakosti (4.22)

$$\begin{aligned} &\lim_{n\to\infty} P(Z_n = z | C_n = c) = \\ &\quad = \lim_{n\to\infty} \sum_{j=0}^{k-1} P(A_n = j) \sum_{i=1}^{k!} P\left(g_{n-1} = f_c^{-1} \circ \Pi_i\right) \cdot P(\Pi_i(j) = z) \\ &\quad = \sum_{j=0}^{k-1} P(A_n = j) \sum_{i=1}^{k!} P(\Pi_i(j) = z) \cdot \lim_{n\to\infty} P\left(g_{n-1} = f_c^{-1} \circ \Pi_i\right) = \end{aligned}$$

$$= \sum_{j=0}^{k-1} P(A_n = j) \sum_{i=1}^{k!} P(\Pi_i(j) = z) \cdot \frac{1}{k!}$$
$$= \frac{1}{k!} \sum_{j=0}^{k-1} P(A_n = j) \sum_{i=1}^{k!} P(\Pi_i(j) = z)$$
$$= \frac{1}{k!} \sum_{j=0}^{k-1} P(A_n = j) \cdot (k-1)! =$$
$$= \frac{(k-1)!}{k!} \sum_{j=0}^{k-1} P(A_n = j) = \frac{1}{k}$$

čime je tvrđenje dokazano.

2. Po definiciji uzajamne količine informacija dve slučajne promenljive imamo da je

$$I(Z_n, C_n) = H(Z_n) - H(Z_n \mid C_n). \tag{4.23}$$

Izračunajmo prvo $H(Z_n)$.

$$H(Z_n) = \sum_{i=0}^{k-1} P(Z_n = i) \log_2 \frac{1}{P(Z_n = i)} \tag{4.24}$$

Prelazeći na limes na obe strane jednakosti (4.24), koristeći činjenicu da je $x \log_2 \frac{1}{x}$ neprekidna funkcija na $(0,1)$ i tvrđenje Teoreme 25 imamo

$$\lim_{n\to\infty} H(Z_n) = \log_2 k. \tag{4.25}$$

Na isti način za $H(Z_n \mid C_n)$ dobijamo

$$H(Z_n \mid C_n) = \sum_{i=0}^{m-1} P(C_n = i) \cdot H(Z_n | C_n = i) = \tag{4.26}$$
$$= \sum_{i=0}^{m-1} P(C_n = i) \cdot \sum_{j=0}^{k-1} P(Z_n = j | C_n = c_i) \log_2 \frac{1}{P(Z_n = j | C_n = i)}$$

i prelazeći na limes u (4.26) uz korišćenje Teoreme 29 tvrđenje 1 dobijamo

$$\lim_{n\to\infty} H(Z_n|C_n) =$$
$$= \sum_{i=0}^{m-1} P(C_n = i) \cdot \sum_{j=0}^{k-1} \lim_{n\to\infty} P(Z_n = j \mid C_n = i) \cdot \lim_{n\to\infty} \log_2 \frac{1}{P(Z_n = j \mid C_n = i)} \tag{4.27}$$

$$= \sum_{i=0}^{m-1} P\left(C_n = i\right) \cdot \sum_{j=0}^{k-1} \frac{1}{k} \log_2 k = \log_2 k \cdot \sum_{i=0}^{m-1} P\left(C_n = i\right) = \log_2 k.$$

Primenom (4.25) i( 4.27) u ( 4.23) sledi

$$\lim_{n\to\infty} I\left(Z_n, C_n\right) = \lim_{n\to\infty} H\left(Z_n\right) - \lim_{n\to\infty} H\left(Z_n|C_n\right) = \log_2 k - \log_2 k = 0 \quad (4.28)$$

čime je i drugo tvrđenje dokazano. ■

**Teorema 30** *[115] Pod uslovima Teoreme 25 važi*

1. $\lim_{n\to\infty} P\left(Z_n = z \,|\, A_n = a\right) = \frac{1}{k}$
2. $\lim_{n\to\infty} I\left(Z_n, A_n\right) = 0$

*za sve* $z, a \in I_k$.

**Dokaz.**

1. Na osnovu definicije uslovne verovatnoće imamo

$$\begin{aligned} &P\left(Z_n = z \,|\, A_n = a\right) = \\ &= \frac{P\left(Z_n = z \wedge A_n = a\right)}{P\left(A_n = a\right)} = \frac{P\left(g_n\left(A_n\right) = z \wedge A_n = a\right)}{P\left(A_n = a\right)} \\ &= \frac{P\left(\left(\bigcup_{i=1}^{k!} g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge A_n = a\right)}{P\left(A_n = a\right)} \\ &= \frac{P\left(\left(\bigcup_{i=1}^{k!} g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge A_n = a\right)}{P\left(A_n = a\right)} \\ &= \frac{P\left(\bigcup_{i=1}^{k!} \left(\left(\left(g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge A_n = a\right)\right)\right)}{P\left(A_n = a\right)}. \end{aligned} \quad (4.29)$$

Kako su događaji

$$\left(\left(\left(g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge A_n = a\right)\right)$$

i

$$\left(\left(\left(g_n = \Pi_j \wedge \Pi_j\left(A_n\right) = z\right) \wedge A_n = a\right)\right)$$

disjunktni kada je $i \neq j$ iz (4.29) dobijamo da je

$$\begin{aligned} &P\left(Z_n = z \,|\, A_n = a\right) = \\ &= \frac{P\left(\bigcup_{i=1}^{k!} \left(\left(\left(g_n = \Pi_i \wedge \Pi_i\left(A_n\right) = z\right) \wedge A_n = a\right)\right)\right)}{P\left(A_n = a\right)} \\ &= \frac{\sum_{i=1}^{k!} P\left(\left(g_n = \Pi_i \wedge \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right)\right)}{P\left(A_n = a\right)}. \end{aligned} \tag{4.30}$$

Primenjujući $P\left(A \wedge B\right) = P\left(A|B\right) \cdot P\left(B\right)$ u (4.30) dobijamo da je

$$\begin{aligned} &P\left(Z_n = z \,|\, A_n = a\right) = \\ &= \frac{\sum_{i=1}^{k!} P\left(\left(g_n = \Pi_i \wedge \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right)\right)}{P\left(A_n = a\right)} \\ &= \frac{\sum_{i=1}^{k!} P\left(g_n = \Pi_i \,|\, \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right) \cdot P\left(\Pi_i\left(a\right) = z \wedge A_n = a\right)}{P\left(A_n = a\right)} \end{aligned} \tag{4.31}$$

$$\begin{aligned} &= \sum_{i=1}^{k!} P\left(g_n = \Pi_i \,|\, \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right) \cdot \frac{P\left(\Pi_i\left(a\right) = z \wedge A_n = a\right)}{P\left(A_n = a\right)} \\ &= \sum_{i=1}^{k!} P\left(g_n = \Pi_i \,|\, \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right) \cdot P\left(\Pi_i\left(A_n\right) = z \,|\, A_n = a\right). \end{aligned}$$

Sada, kako su $\{g_n = \Pi_i\}$ i $\{\Pi_i\left(A_n\right) = z \wedge A_n = a\}$ nezavisne slučajne promenljive primenom u (4.31) dobijamo

$$\begin{aligned} &P\left(Z_n = z \,|\, A_n = a\right) = \\ &= \frac{\sum_{i=1}^{k!} P\left(\left(g_n = \Pi_i \wedge \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right)\right)}{P\left(A_n = a\right)} \\ &= \frac{\sum_{i=1}^{k!} P\left(g_n = \Pi_i | \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right) \cdot P\left(\Pi_i\left(a\right) = z \wedge A_n = a\right)}{P\left(A_n = a\right)} = \end{aligned} \tag{4.32}$$

$$= \sum_{i=1}^{k!} P\left(g_n = \Pi_i \,|\, \left(\Pi_i\left(A_n\right) = z \wedge A_n = a\right)\right) \cdot P\left(\Pi_i\left(A_n\right) = z \,|\, A_n = a\right)$$

$$= \sum_{i=1}^{k!} P\left(g_n = \Pi_i\right) \cdot P\left(\Pi_i\left(a\right) = z\right)$$

uzimajući limes na obe strane jednakosti (4.32) sledi

$$\begin{aligned}
&\lim_{n\to\infty} P\left(Z_n = z \,|\, A_n = a\right) = \\
&\quad = \lim_{n\to\infty} \sum_{i=1}^{k!} P\left(g_n = \Pi_i\right) \cdot P\left(\Pi_i\left(a\right) = z\right) \\
&\quad = \sum_{i=1}^{k!} \lim_{n\to\infty} P\left(g_n = \Pi_i\right) \cdot P\left(\Pi_i\left(a\right) = z\right) \\
&\quad = \sum_{i=1}^{k!} \frac{1}{k!} \cdot P\left(\Pi_i\left(a\right) = z\right) \\
&\quad = \frac{1}{k!} \sum_{i=1}^{k!} P\left(\Pi_i\left(a\right) = z\right) \\
&\quad = \frac{1}{k!} \cdot (k-1)! = \frac{1}{k}
\end{aligned}$$

čime je tvrđenje dokazano.

2. Na isti način kao u Teoremi 29 dobijamo da je

$$\lim_{n\to\infty} H\left(Z_n\right) = \log_2 k$$

Koristeći definiciju uslovne entropije imamo

$$\begin{aligned}
H\left(Z_n \,|\, A_n\right) &= \sum_{i=0}^{k-1} P\left(A_n = i\right) \cdot H\left(Z_n \,|\, A_n = i\right) \qquad (4.33) \\
&= \sum_{i=0}^{k-1} P\left(A_n = i\right) \cdot \sum_{j=0}^{k-1} P\left(Z_n = j \,|\, A_n = i\right) \log_2 \frac{1}{P\left(Z_n = j \,|\, A_n = i\right)}
\end{aligned}$$

Prelazeći na limes na obe strane jednakosti u (4.33), koristeći Teoremu 30 tvrđenje 1 i činjenicu da je $x \log_2 \frac{1}{x}$ neprekidna funkcija na $(0,1)$ sledi

$$\begin{aligned}
&\lim_{n\to\infty} H\left(Z_n \,|\, A_n\right) = \\
&= \sum_{i=0}^{k-1} P\left(A_n = i\right) \cdot \sum_{j=0}^{k-1} \lim_{n\to\infty} P\left(Z_n = j \,|\, A_n = i\right) \cdot \lim_{n\to\infty} \log_2 \frac{1}{P\left(Z_n = j \,|\, A_n = i\right)}
\end{aligned} \qquad (4.34)$$

$$= \sum_{i=0}^{k-1} P(A_n = i) \cdot \sum_{j=0}^{k-1} \frac{1}{k} \log_2 k = \log_2 k \cdot \sum_{i=0}^{k-1} P(A_n = i) = \log_2 k$$

Uvrstivši (4.25) i (4.34) u definiciju za $I(Z_n, A_n)$ dobijamo

$$\lim_{n\to\infty} I(Z_n, A_n) = \lim_{n\to\infty} H(Z_n) - \lim_{n\to\infty} H(Z_n|A_n) = \log_2 k - \log_2 k = 0$$

što dokazuje drugo tvrđenje. ■

## 4.2 Klasa pseudoslučajnih generatora sa promenljivim permutacijama

Teorija pseudoslučajnih generatora, skraćeno PSG, se u zavisnosti od modela kojim se procenjuje njegova kriptografska bezbednost definiše na različite načine o čemu je bilo reči u poglavlju 2.4 glave 2. U ovom delu ćemo kriptografsku bezbednost pseudoslučajnog generatora razmatrati u skladu sa pristupom opisanim 2.6 poglavlja 2.

Pseudoslučajne generatore ćemo posmatrati kao konačne automate sa izlazom. Pseudoslučajni generator $R$ nad skupom simbola $I_k$ kod kojeg posmatramo samo izlazni niz ćemo identifikovati uređenim parom $(s_R, \{R_i\}_{i=0}^{\infty})$. Niz $\{R_i\}_{i=0}^{\infty}$ je izlazni niz pseudoslučajnog generatora $R$ a vrednost $s_R$, parametar koji determiniše izlazni niz $\{R_i\}_{i=0}^{\infty}$, je ključ pseudoslučajnog generatora $R$. Kako je pseudoslučajni generator $R$ konačan automat sa izlazom to je izlazni niz nužno periodičan i njegov period označimo sa $p_R$, tada je

$$P(R_i = l) = \frac{|\{m \,|\, R_m = l,\, 0 \le m < p_R\}|}{p_R},\ l \in I_k$$

Definišimo sada klasu pseudoslučajnih generatora sa promenljivim permutacijama

**Definicija 31** *Neka je dat skup $S = \{f_0, f_1, \ldots, f_{m-1}\} \subseteq \mathcal{P}_k$ i dva nezavisna pseudoslučajna generatora, $A = (s_A, \{A_n\}_{n=1}^{\infty})$ nad skupom simbola $I_k$ i $C = (s_C, \{C_n\}_{n=1}^{\infty})$ nad skupom simbola $I_m$. Definišimo sada klasu pseudoslučajnih generatora sa promenljivim permutacijama $Z = ((s_A, s_C), \{Z_n\}_{n=1}^{\infty})$ na sledeći način:*

$$\begin{aligned} g_0 &= p & p &\in \mathcal{P}_k \\ g_{n+1} &= f_{C_{n+1}} \circ g_n & n &\ge 0 \\ Z_{n+1} &= g_{n+1}(A_{n+1}) & n &\ge 0. \end{aligned} \tag{4.35}$$

*gde je $(s_A, s_C)$ ključ pseudoslučajnog generatora $Z$.*

Za pseudoslučajni generator $Z$ kažemo da je parametrizovan pseudoslučajnim generatorima $A$ i $C$. Iako su definicija 24 na strani 90 i definicija 31 gotovo identične po formulaciji razlika je suštinska u prirodi parametrizujućih sekvenci. U prvom slučaju reč je o slučajnim procesima a u drugom o pseudoslučajnim nizovima.

U imenovanju ovog modela koristićemo i termin generički sa značenjem da je model parametrizovan sa dva pseudoslučajna niza i da se upotrebom konkretnih pseudoslučajnih nizova odgovarajućih karakteristika dobijaju kriptografski dobri pseudoslučajni generatori.

## 4.3 Kriptografske bezbednosne karakteristike definisane klase generatora

Kriptografske bezbednosne karakteristike definisanog pseudoslučajnog generatora ćemo razmatrati u skladu sa pristupom opisanim u poglavlju 2.6 glave 2 i osobinama koje su uzrok kompromitacije pseudoslučajnog generatora RC4 opisanim u glavi 3.

Prilikom ovih bezbednosnih analiza a u skladu sa određenjem napada, kako je to opisano u delu 2.4, za napadača ćemo pretpostaviti da procesna snaga u klasi složenosti $PPT$ i da su mu sposobnosti na nivou poznavanja jednog dela izlaznog niza. Za aditivne sekvencijalne kriptografske algoritme ovim su obuhvaćeni napadi klasa CPA i KPA, deo 2.4 strana 2.

### 4.3.1 Period izlaznog niza

Sa stanovišta kriptografske sigurnosti jedna od bitnih karakteristika pseudoslučajnih generatora je da su njihovi izlazni nizovi periodični. Veličina perioda pseudoslučajnog niza u aditivnim sekvencijalnim kriptografskim algoritmima utiče na mogućnost sprovođenja napada na sistem Kerhofsovom metodom i da bi se taj tip napada onemogućio zahteva se da izlazni nizovi pseudoslučajnih generatora imaju periode čija je veličina veoma velika.

Dakle imamo da su $\{A_n\}_{n=1}^{\infty}$, $\{C_n\}_{n=1}^{\infty}$ periodični i označimo njihove periode sa $p_A$ i $p_C$ respektivno. Kako je $(\mathcal{P}_k, \circ)$ konačna grupa lako se pokazuje da je i niz $\{g_n\}_{n=0}^{\infty}$, periodičan. Kako su $\{A_n\}_{n=1}^{\infty}$, $\{C_n\}_{n=1}^{\infty}$ i $\{g_n\}_{n=0}^{\infty}$ periodični nizovi

to i $\{Z_n\}_{n=1}^{\infty}$ mora biti periodičan. Označimo periode nizova $\{g_n\}_{n=0}^{\infty}$ i $\{Z_n\}_{n=1}^{\infty}$ sa $p_G$, $p_Z$ respektivno.

Period $p_Z$ izlaznog niza $\{Z_n\}_{n=1}^{\infty}$ odredićemo u nekoliko koraka.

Prvo ćemo odrediti period $p_G$ niza $\{g_n\}_{n=0}^{\infty}$.

**Lema 32** *Neka je* $l \in \mathbb{N}$ *red permutacije* $\prod_{i=1}^{p_C} f_{C_{p_C-i+1}}$ *u grupi* $(\mathcal{P}_k, \circ)$. *Tada je period niza* $\{g_n\}_{n=0}^{\infty}$ *dat sa* $p_g = lp_C$.

**Dokaz.** Lako se pokazuje da je $lp_C$ period niza $\{g_n\}_{n=0}^{\infty}$.

$$g_{k+\lambda l p_C} = f_{C_{k+\lambda lC}} \circ \ldots \circ f_{C_{1+\lambda lC}} \circ f_{C_{\lambda lC}} \circ \ldots \circ f_{C_2} \circ f_{C_1}$$

a pošto je $p_C$ period niza $\{C_n\}_{n=1}^{\infty}$ imamo

$$\begin{aligned} & f_{C_{k+\lambda lC}} \circ \ldots \circ f_{C_{1+\lambda lC}} \circ f_{C_{\lambda lC}} \circ \ldots \circ f_{C_2} \circ f_{C_1} = \\ & = \left(f_{C_{p_C}} \circ \ldots \circ f_{C_2} \circ f_{C_1}\right)^{\lambda l} \circ f_{C_k} \circ \ldots \circ f_{C_1} \\ & = f_{C_k} \circ \ldots \circ f_{C_1} \\ & = g_k \end{aligned}$$

i $lp_C$ je period.

Dokažimo sada da je $lp_C$ osnovni period odnosno da je svaki drugi period niza $\{g_n\}_{n=0}^{\infty}$ je deljiv sa $lp_C$.

Pretpostavimo suprotno, da $lp_C$ nije osnovni period. To znači da postoji broj $d \in \mathbb{N}$ koji je osnovni period i važi $d \,|\, lp_C$ i $d < lp_C$. Iz

$$g_{k+\lambda d} = g_k$$

dobijamo

$$\prod_{i=k+\lambda d}^{k+1} f_{C_i} = I,\ k \in \mathbb{N}, k \geq 1 \tag{4.36}$$

gde je $I$ jedinična permutacija. Množeći (4.36) sa desne strane permutacijom $f_{C_k}$ dobijamo

$$f_{C_{k+\lambda d}} \circ \prod_{i=k+\lambda d-1}^{k} f_{C_i} = f_{C_k}.$$

Primenjujući (4.36) dobijamo

$$f_{C_{k+\lambda d}} = f_{C_k},\ k \geq 1.$$

Kako su $f_{C_{k+\lambda d}}, f_{C_k}$ permutacije i zbog uslova 2. u (4.1) imamo

$$C_{k+\lambda d} = C_{k,} \quad k \geq 1$$

što znači da je $d$ period niza $\{C_n\}_{n=1}^{\infty}$ i da $p_C \,|\, d$ odnosno. $d = rp_C$, $r < l$.
Posmatrajmo sada $g_{1+\lambda d}$

$$g_{1+\lambda d} = \prod_{i=1+\lambda d}^{1} f_{C_i} = f_{C_{1+\lambda r p_C}} \circ \prod_{i=\lambda r p_C}^{1} f_{C_i} =$$
$$= f_{C_1} \circ \left( \prod_{i=p_C}^{1} f_{C_i} \right)^{\lambda r} = f_{C_1} = g_1$$

Odakle zaključujemo da je

$$\left( \prod_{i=p_C}^{1} f_{C_i} \right)^{\lambda r} = I$$

za svako $\lambda \geq 1$. Konačno stavljajući $\lambda = 1$ dobijamo

$$\left( \prod_{i=1}^{C} f_{C_i} \right)^{r} = I$$

Odakle sledi da $l \,|\, r$ što nije moguće jer je $r < l$. Ova kontradikcija pokazuje da je $lp_C$ osnovni period niza $\{g_n\}_{n=0}^{\infty}$ i lema je dokazana. ■

**Lema 33** *Neka je $p_G$ osnovni period niza $\{g_n\}_{n=0}^{\infty\infty}$. Ako je $(p_G, p_A) = 1$ i $\{A_1, A_2, \ldots, A_n, \ldots\} = I_k$ tada je $p_G\, p_A$ period niza $\{Z_n\}_{n=1}^{\infty}$.*

**Dokaz.** Direktnom proverom se lako dobija da je $p_G\, p_A$ period niza$\{Z_n\}_{n=1}^{\infty}$. Treba još pokazati da je $p_G\, p_A$ osnovni period niza $\{Z_n\}_{n=1}^{\infty}$.
Pretpostavimo da je osnovni period jednak $d \neq p_G\, p_A$. Tada $d \mid p_G\, p_A$ i pošto je $(p_G,\, p_A) = 1$ imamo da je

$$d = d_1 d_2, \quad (d_1, d_2) = 1 \tag{4.37}$$

i još

$$d_1 \,|\, p_G,\ d_2 \,|\, p_A$$

Kako je $d$ period niza $\{Z_n\}_{n=1}^{\infty}$ imamo,

$$g_{k+\lambda d}\,(A_{k+\lambda d}) = g_k\,(A_k) \tag{4.38}$$

za svako $\lambda \geq 1, \lambda \in \mathbb{N}$. Stavimo da je $\lambda = \lambda_1 \cdot \frac{p_G}{d_1}, \lambda_1 \geq 1$ u (4.5) čime dobijamo

$$g_{k+\lambda_1 p_G d_2}\left(A_{k+\lambda_1 p_G d_2}\right) = g_k\left(A_k\right).$$

Kako je $p_G$ period $\{g_n\}_{n=0}^{\infty}$ dobijamo

$$g_k\left(A_{k+\lambda_1 p_G d_2}\right) = g_k\left(A_k\right).$$

Kako je $g_k$ bijektivna transformacija dobijamo

$$A_{k+\lambda_1 p_G d_2} = A_k$$

što znači da je $p_G d_2$ period niza $\{A_n\}_{n=1}^{\infty}$ i posledično $p_A \,|\, p_G d_2$. Kako je $(p_G, p_A) = 1$ dobijamo da $p_A \,|\, d_2$ što sa $d_2 | p_A$ daje $p_A = d_2$. Sada, prema (4.37) mora biti $d = d_1 p_A$. Zamenjujući u (4.38) dobijamo

$$g_{k+\lambda d_1 p_A}\left(A_{k+\lambda d_1 p_A}\right) = g_k\left(A_k\right).$$

Što se svodi na

$$g_{k+\lambda d_1 p_A}\left(A_k\right) = g_k\left(A_k\right)$$

jer je $p_A$ period niza $\{A_n\}_{n=1}^{\infty}$.
Posmatrajmo sada $g_{k+np_G+\lambda d_1 p_A}\left(A_{k+np_G+\lambda d_1 p_A}\right)$.

$$\begin{aligned} g_{k+\lambda d_1 p_A}\left(A_{k+np_G}\right) &= g_{k+np_G+\lambda d_1 p_A}\left(A_{k+np_G+\lambda d_1 p_A}\right) = \\ &= g_{k+np_G}\left(A_{k+np_G}\right) = \\ &= g_k\left(A_{k+np_G}\right) \end{aligned}$$

što znači da su funkcije $g_{k+\lambda d_1 p_A}\left(A_{k+np_G}\right)$, $g_k\left(A_{k+np_G}\right)$ jednake na skupu $\{A_{k+np_G} \mid n \in \mathbb{N}\}$. Skup $\{x \mid k + np_G \equiv_{p_A} x,\ n \in \mathbb{N}\}$ je jednak skupu $I_{p_A}$, jer je $(p_G, p_A) = 1$, odakle sledi da je $\{A_{k+np_G} \mid n \in \mathbb{N}\} = I_k$. Funkcije $g_{k+\lambda d_1 A}$, $g_k$ su jednake na svojim domenima pa imamo

$$g_{k+\lambda d_1 p_A} = g_k\ , \lambda \geq 1, \lambda \in \mathbb{N}$$

odakle sledi da je $d_1 p_A$ period niza $\{g_n\}_{n=0}^{\infty}$. Slično kao prethodno zaključujemo da je $d_1 = p_G$ a odatle imamo da je osnovni period niza $\{Z_n\}_{n=1}^{\infty}$ $p_G p_A$. ■

Sledeće tvrđenje je trivijalna posledica leme 33.

**Posledica 34** *[115] Ako je* $(p_G, p_A) = 1$ *tada je period niza* $\{Z_n\}_{n=1}^{\infty}$ *veći ili jednak od* $p_A$.

Sledeća teorema daje dovoljne uslove, u terminima nizova $\{A_n\}_{n=1}^{\infty}$, $\{C_n\}_{n=1}^{\infty}$ kada se period izlaznog niz povećava u odnosu na parametrizujuće nizove.

**Teorema 35** *[115] Neka je $l \in \mathbb{N}$ red permutacije $\prod_{i=1}^{p_C} f_{C_{p_C-i+1}}$ u grupi $(\mathcal{P}_k, \circ)$. Ako je $(lp_C, p_A) = 1$ i $\{A_1, A_2, \ldots, A_n, \ldots\} = I_k$, period niza $\{Z_n\}_{n=1}^{\infty}$ je*

$$p_Z = l \cdot p_C \cdot p_A$$

Teorema 35 je direktna posledica prethodno dokazanih lema.

### 4.3.2 Statistička i korelaciona analiza

Statističkom i korelacionom analizom se utvrđuju probabilističke karakteristike pseudoslučajnog generatora i njihov uticaj na prediktabilnost izlaznog niza. Prilikom ove analize smatraćemo da su parametrizujući pseudoslučajni generatori $A$ i $C$ odabrani tako da

$$\begin{aligned} &1. \quad \sum_{l=0}^{k-1} P(A_i = l) = 1 \quad i \quad P(A_i = l) > 0 \quad za \quad sve \quad l \in I_k, \\ &2. \quad \sum_{l=0}^{m-1} P(C_i = l) = 1 \quad i \quad P(C_i = l) > 0 \quad za \quad sve \quad l \in I_m, \end{aligned} \tag{4.39}$$

#### 4.3.2.1 Raspodela verovatnoća izlaznog niza

Jednakosti date u (4.39) obezbeđuju važenje teoreme 25 odakle zaključujemo da izlazni niz pseudoslučajnog generatora $Z$ ima asimptotski uniformnu raspodelu. Drugim rečima postoji $n_0 \in \mathbb{N}$ tako da kada je $n > n_0$ tada je za svako $l \in I_k$ razlika $\left|P(Z_i = l) - \frac{1}{k}\right|$ proizvoljno mala. Ako sa $\varepsilon$ označimo sigurnosnu marginu, vrednost kada smatramo da je razlika između uniformne raspodele i raspodele verovatnoća pseudoslučajnog niza $Z$ nebitna, tada za elemente izlaznog niza $Z_n$ kod kojih je $n > n_0(\varepsilon)$ smatramo da imaju uniformnu raspodelu. Određivanje broja $n_0(\varepsilon)$ zavisi od izabranog skupa $S$ i realizuje se u svakom konkretnom slučaju posebno.

Da bi se dobila uniformna raspodela u izlaznom nizu $\{Z_n\}_{n=1}^{\infty}$ dovoljno je odabrati pseudoslučajni generator $A$ tako da elementi njegovog izlaznog niza imaju uniformnu raspodelu, Teorema 27.

U glavi 3 je pokazano da u generatoru RC4 raspodela verovatnoća za izlazni niz nije ni asimptotski uniformna jer se vrednost $P(z_r = 0)$ statistički značajno razlikuje od $\frac{1}{N}$, videti glavu 3 nejednakost (3.16) strana 80. Za definisani generator je pokazano da takvih slabosti nema.

Treba istaći da su u analizama raspodele verovatnoća izlaznog niza pseudoslučajnog generatora, generalno, retke situacije kada postoje dokazi ravnomernosti te raspodele, ili pak ako ih ima pretpostavljaju ravnomerne raspodeljenosti verovatnoća komponenti unutrašnjeg stanja generatora pseudoslučajnog niza
Za klasu generatora datu definicijom 31 to nije tako. Pseudoslučajni nizovi $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$ koji čine unutrašnje stanje definisanog generatora mogu imati funkcije raspodele verovatnoća koje drastično odstupaju od ravnomerne raspodele, samo moraju biti potpune u smislu da se pojavljuju sve vrednosti iz skupa $I_k$, uslov (4.39).

Na osnovu prethodno iznetog definisana klasa pseudoslučajnih generatora ima dobre osobine u pogledu raspodele verovatnoća elementa izlaznog niza.

#### 4.3.2.2 Korelaciona analiza

U glavi 3 je pokazano da u izlaznom nizu pseudoslučajnog generatora RC4 postoje bliske i udaljene korelacije kao i da se pojavljuju proizvoljno daleko u generisanom izlaznom nizu. Prikazane korelacije imaju potencijal kompromitovanja generatora RC4.

Za definisanu klasu pseudoslučajnih generatora izvedeni su dovoljni uslovi pod kojim izlazni niz nema ni bliske ni udaljene korelacije, Teorema 28. Posledica ove činjenice je da poznavanje odsečka izlaznog niza ne omogućava predikciju budućih elemenata izlaznog niza.

Sledeće važno pitanje je postojanje korelacije između izlaznog niza $\{Z_n\}_{n=1}^{\infty}$ i vrednosti $s_A$ i $s_C$,drugim rečima postojanje korelacije između izlaznog niza pseudoslučajnog generatora i njegovog ključa. Teoremom 29 je pokazano da su $A_n$ i $Z_n$ asimptotski nezavisne veličine a Teoremom 30 da su $C_n$ i $Z_n$ asimptotski nezavisne veličine. Posledica toga je da $\lim_{n\to\infty} I(Z_n, A_n) = \lim_{n\to\infty} I(Z_n, C_n) = 0$ što znači da se količina informacija o ključu koju nosi izlazni niz može učiniti proizvoljno malom i prema tome bezopasnom po definisanu klasu generatora, na primer odbacivanjem početnog odsečka određene dužine.

U slučaju da $\{A_n\}_{n=1}^{\infty}$ i $\{C_n\}_{n=1}^{\infty}$ imaju ravnomerne raspodele asimptotske relacije postaju egzaktne relacije.

Na osnovu prethodno iznetog definisana klasa pseudoslučajnih generatora ima dobre osobine u pogledu korelacionih osobina izlaznog niza unutrašnjih stanja i ključeva.

### 4.3.3 Algebarska analiza definisanog generatora

Algebarska analiza razmatra mogućnosti uspešnog napada na kriptografski algoritam primenom algebarskih metoda. Cilj napadača može biti:

- Da algebarskim tehnikama razloži kriptografski algoritam na autonomne celine i potom pojedinačnom analizom pokuša da dođe do rezultata.
- Da oformi algebarski sistem jednačina koji opisuje kriptografski algoritam i na osnovu izlaznog niza da ga reši te tako dođe do primenjenog kriptografskog ključa.

Prvi pristup ne deluje perspektivno iz sledećih razloga. Ako bi takav pristup bio moguć to bi značilo da se skup $\mathcal{P}_k$ može razbiti na nekoliko particija $S_1, S_2, ..., S_l$ tako da je

$$\begin{aligned} &\mathcal{P}_k = S_1 \cup S_2 \cup \cdots \cup S_l \ , \quad l \geq 2 \\ &S_i \cap S_j = \varnothing, \ S_i, S_j \neq \varnothing, \quad i \neq j \end{aligned} \tag{4.40}$$

i takvo razbijanje mora biti stabilno u smislu da

$$f_i \in S \wedge s \in S_j \Longrightarrow f_i \circ s \in S_j \tag{4.41}$$

za svako $i \in I_k$ i $j \in I_l$.
Međutim takvo razbijanje nije moguće što se vidi na sledeći način.
Neka je $i_0$ indeks takav da $\Pi_1 \in S_{i_0}$. Tada, pošto je $\Pi_1 \circ f_l = f_l$ za svako $f_l \in S$ sledi da će posle nekog vremena biti $S \subseteq S_{i_0}$ zbog (4.41). Sada se indukcijom zaključuje da će za svako $k$ biti $S^k \subseteq S_{i_0}$. Kako je $\langle S \rangle = \mathcal{P}_k$ to je onda $S_{i_0} = \mathcal{P}_k$ što znači da razbijanje (4.40) ne postoji i takav pristup nije moguć.

Drugi pristup je moguć ali dobijeni sistem jednačina verovatno ne bi bio efektivno rešiv. Heuristički razlozi su sledeći. Definisani generički model pseudoslučajnog generatora je složeniji po svojoj strukturi od RC4 jer je parametrizovan sa dva pseudoslučajna generatora i operacija promene permutacija nije jednostavnija od one u RC4. Stoga je očekivano da sistem algebarskih jednačina koji odgovora

definisanom generatoru bude složeniji od sistema jednačina koji odgovara RC4, barem po broju promenljivih i broju jednačina. Ovaj pristup za generator RC4 sa $N = 8$ daje sistem sa 532480 nepoznatih i 534536 jednačina nad $\mathbb{F}_2$, [119]. Kako za rešavanje nelinearnih sistema jednačina u konačnim poljima nije poznat algoritam za rešavanje bitno brži od potpune pretrage to je složenost izvršavanja algoritma za nalaženje rešenja ovog sistema jednačina uporediva sa $2^{532480}$ što je nedostižan zadatak. Shodno tome ni zadatak rešavanja sistema jednačina koji odgovara definisanoj klasi generatora nije ostvariv.

## 4.4 Primene definisane klase pseudoslučajnih generatora

Potreba za uspostavljanjem pouzdanih mehanizama bezbednosti u sajber prostoru je doprinela da se proučavanje sekvencijalnih kriptografskih algoritama nađe u fokusu današnje kriptografije. Nekoliko je izvorišta upotrebljivosti sekvencijalnih kriptografskih algoritama u bezbednosnim rešenjima zaštite informacionih sistema i podataka. Inicijalno to se odnosi na lakoću hardverske i softverske implementacije ali dominantni su bezbednosni razlozi. Sekvencijalni kriptografski algoritmi koriste relativno kratke kriptografske ključeve što olakšava njihovo generisanje, distribuciju i upravljanje njima. U isto vreme dobro dizajnirani sekvencijalni kriptografski algoritmi nude vrlo visok nivo bezbednosti. Sve ovo, prethodno nabrojano, je od esencijalne važnosti za njihovu primenljivost i upotrebu.

### 4.4.1 Primena u sintezi sekvencijalnih kriptografskih algoritama

Sinteza sekvencijalnih kriptografskih algoritama predstavlja složen i odgovoran istraživački zadatak. Do sada nije razvijena metodologija sinteze sigurnih sekvencijalnih algoritama kao na primer u slučaju blokovskih kriptografskih algoritama, [62], [122], [64]. Ko što smo videli u delu 2.3 poglavlja 2 neke funkcionalne celine u strukturi pouzdanih sekvencijalnih kriptografskih algoritma se mogu izdvojiti ali njihova upotreba ne garantuje postizanje zadovoljavajućeg nivoa bezbednosti.

Definisana klasa pseudoslučajnih generatora ima dobre kriptografske bezbednosne karakteristike i njena upotreba u aditivnim sekvencijalnim kriptografskim

algoritmima ima potencijal da produkuje bezbedne kriptografske algoritme. U ovom obliku primena je prevashodno orjentisana na uređaje sa ograničenim računarskim resursima.

Ova klasa pseudoslučajnih generatora takođe može biti upotrebljena kao gradivni element pri sintezi složenijih kriptografskih algoritama zbog svojih dobrih bezbednosnih osobina na sličan način kao što se koriste Bulove funkcije. linearni pomerački registri, filter generator i slične strukture. Mora se naglasiti da upotreba definisane klase u nekoj konstrukciji ne znači nužno dobre bezbednosne karakteristike konstrukcije po sebi. Svaka takva konstrukcija mora biti podvrgnuta detaljnoj i dubokoj bezbednosnoj analizi kako bi se njene bezbednosne osobine utvrdile. Brojni su primeri loših konstrukcija nastalih upotrebom dobrih elemenata, [15], [116], [50].

### 4.4.2 Primena u sintezi slučajnih generatora

Jedan od fundamentalnih principa moderne kriptografije je Kerhofsov princip, [56], [57], koji postulira da šifrati pouzdanog kriptografskog algoritma moraju biti sigurni čak i kada su sve informacije o kriptografskom algoritmu, osim upotrebljenog ključa, poznate protivniku. Drugačije rečeno, sigurnost podataka počiva na protivnikovom nepoznavanju upotrebljenog ključa. Protivnikovo nepoznavanje ključa podrazumeva i mogućnosti njegovog pogađanja ili rekonstrukcije. Da bi se to izbeglo ključ mora biti generisan na slučajan način i mora imati dovoljnu dužinu kako bi potpuna pretraga po svim mogućim ključevima bila neizvodljiva. U tom kontekstu osnovni problem je generisanje ključa na slučajan način odnosno pristup generatoru slučajnih brojeva. Generatori slučajnih brojeva su procesi čiji ishodi imaju karakteristike neprediktabilnosti u smislu da poznavanje istorije procesa ne određuje njegove buduće ishode. Po svojoj prirodi oni mogu biti:

- Fizički, kada koriste prirodne fenomene čiji ishodi predstavljaju slučajne procese, na primer vremenske intervale između emisije čestica radioaktivnih elemenata, termalni šum elektronskih elemenata i drugo.
- Nefizički, kada se kao izvor slučajnosti koriste događaje u ljudskoj interakciji, informacionim sistemima i drugo, na primer vremenski intervali između pritiskanja tipki na tastaturi, adrese pristupa sektorima na hard disku, treptaji očnih kapaka i drugo.

U prvom slučaju se koriste procesi koji imaju uniformnu raspodelu i iz te uniformnosti rezultuje neprediktabilnost ishoda. U praksi se može desiti da uniformnost raspodele događaja bude narušena iz raznih razloga, od uticaja merne aparature na sam proces do nepreciznosti merne aparature.

U drugom slučaju entropija događaja najčešće nije velika i uniformnost raspodele i neprediktabilnost ishoda se postiže dodatnim matematičkim transformacijama.

Definisana klasa generatora omogućava da se iz uzoraka kod kojih je narušena uniformnost raspodele dobije uzorak sa uniformnom raspodelom. To se postiže na taj način što se dva nesavršena niza dobijena procesom koji daje uzorke sa raspodelom koja nije ravnomerna propuste kroz definisanu konstrukciju koja kao rezultat daje niz sa uniformnom raspodelom.

Ovde treba uočiti da ova primena funkcioniše i kada generisani uzorci drastično odstupaju od uniformne raspodele zbog Teoreme 25.

## 4.5 Zaključak

Polazeći od zahteva za uspostavljanje bezbednog informacionog okruženja u sajber prostoru i činjenice da taj prostor čine, po svojim računarskim mogućnostima, heterogeni uređaji, IoT i WSN, pojavila se suštinska potreba za definisanjem bezbednog, efikasnog i kompaktnog kriptografskog algoritma. Po svojim karakteristikama u tom smislu se izdvaja klasa sekvencijalnih kriptografskih algoritama. Sinteza pouzdanog, kompaktnog i efikasnog sekvencijalnog kriptografskog algoritma je složen istraživački zadatak. U praksi je primenjeno nekoliko različitih rešanja ali se među njima posebno ističe kriptografski algoritam RC4. Brilijantna ideja, upotreba promenljivih permutacija, i njena efikasna realizacija doveli su do masovne primene ovog kriptografskog algoritma. Na žalost kriptografski algoritam RC4 nije izdržao test vremena i 2015. godine povučan je iz upotrebe. Polazni stav ovog rada je sama primena promenljivih permutacija nije uzrok problema već je to način njene primene. Sprovedena istraživanja rezultirala su definisanjem klase kriptografskih algoritama, definicija 31, sa dobrim kriptografskim osobinama, kompaktnim opisom i mogućnostima efikasne implementacije.

Definisana je klasa pseudoslučajnih generatora bazirana na promenljivim permutacijama koja je parametrizovana sa dva pseudoslučajna niza. Način na koji je klasa definisana omogućava njenu implementaciju na efikasan i kompaktan način.

Sprovedene su analize statističkih, korelacionih i algebarskih bezbednosnih kriptografskih osobina definisane klase. Statistička analiza je pokazala da vrednosti izlaznog niza u opštem slučaju imaju asimptotski ravnomernu raspodelu. Korelaciona analiza je pokazala da ne postoje korelacije između elemenata izlaznog niza a parametri definisanog generatora su asimptotski nezavisni od elemenata izlaznog niza. Korelaciona analiza je takođe pokazala da količina informacija koju izlazni niz nosi o unutrašnjem stanju generatora teži nuli sa vremenom rada generatora. Posledično je i količina informacija koju izlazni niz nosi o primenjenom kriptografskom ključu teži nuli sa vremenom rada generatora. Sprovedena algebarska analiza ne ukazuje na mogućnost kompromitacije ovog generatora do sada poznatim algebarskim metodama.

Dodatno, dati su dovoljni uslovi za parametre definisane klase pseudoslučajnih generatora parametrizovana čija ispunjenost obezbeđuje da asimptotski rezultati u formulama za raspodelu verovatnoća i korelacije,Teorema 25, Teorema 29 i Teorema 30, postaju egzaktni.

Sprovedena analiza je pokazala otpornost definisane klase pseudoslučajnih generatora na ciljeve napadača opisane u poglavlju 2.6 na strani 55 i kriterijume sinteze sekvencijalnih kriptografskih algoritama u istom delu.

Definisana klasa na izvestan način predstavlja uopštenje ideja kriptografskog algoritma RC4 ali eliminiše sve bezbednosne slabosti koje postoje u kriptografskom algoritmu RC4. Bezbednosne karakteristike ove klase kriptografskih algoritama i kompaktnost njeog opisa omogućavaju primenu i u uređajima sa vrlo ograničenim resursima uz postizanje visokog nivoa bezbednosti. Pored primene u sintezi kriptografskih algoritma ova klasa transformacija omogućava realizaciju generatora slučajnih simbola i iz slučajnih procesa koji po svojoj prirodi nemaju uniformnu raspodelu na skupu detektovanih vrednosti.

Bezbednosne karakteristike, kompaktnost i moguća efikasnost implementacije ove klase kriptografskih algoritama, s obziron na širok raspon uređaja u kojima se mogu primeniti, imaju potencijal standardizacije bezbednosnih mehanizama u sajber prostoru.

# Glava 5

# Rezime, doprinosi i otvorena pitanja

## 5.1 Rezime

Napretkom i širenjem komunikacionih i mrežnih tehnologija, kao i tehnološkim napretkom u dizajniranju i primeni mikroprocesorskih uređaja, stvorili su se uslovi za komunikaciono povezivanje različitih uređaja i stvaranja inteligentnih sistema sposobnih za nadgledanje i upravljanje složenim procesima. Sposobnost povezivanja na tehnološkim osnovama Internet infrastrukture, komunikaciona infrastruktura i Internet skup protokola, omogućila je povezivanje mnoštva heterogenih uređaja u funkcionalna okruženja poput bežičnih senzorskih mreža (VSN) i Interneta stvari (IoT). U tom kontekstu, informaciona bezbednost ima veoma važnu ulogu u obezbeđivanju poverljivosti i integriteta podataka, realizaciji pouzdanih protokola autentifikacije i autorizacije te obezbeđivanju neporecivosti za preduzete akcije u sistemu. Pored sigurnosnih mehanizama ugrađenih u Internet protokole dodatni sigurnosni mehanizmi implementiraju se u uređaje radi bezbednosnog obezbeđenja sistemske funkcionalnosti okruženja kojem uređaji pripadaju. U takvim sistemima funkcioniše ogroman broj uređaja (senzori, kamere, nadzorni sistemi) koji moraju da rade u realnom vremenu a da definisani bezbednosni mehanizmi ne narušavaju ponašanje sistema. Kriptologija obezbeđuje teorijsku osnovu za definisanje i implementaciju bezbednosnih rešenja u komunikaciono umreženom svetu.

U radu je dat osnovni pregled kriptoloških pojmova i klasifikacija. Pošto je rad usmeren na sintezu aditivnih sekvencijalnih kriptografskih algoritama u prikazu

kriptografske taksonomije i strukture kriptografskih algoritma pažnja je usmerena na sekvencijalne kriptografske algoritme. Ilustrovana je složenost sinteze kriptografski pouzdanih sekvencijalnih kriptografskih algoritama prikazom nekoliko svetskih konkursa za predloge kriptografskih bezbednosnih rešenja i njihovih rezultata. Njihov relativni neuspeh u sferi sekvencijalnih kriptografskih algoritama svedoči o složenosti sinteze pouzdanih sekvencijalnih kriptografskih algoritama.

U radu su prikazane osnovne gradivne strukture sekvencijalnih kriptografskih algoritama, bezbednosni modeli koji se koriste za procenu njihove kriptografske snage i metodologija sinteze i bezbednosne evaluacije sekvencijalnih kriptografskih algoritama.

Jedan od najintrigantnijih primera u tom smislu je kriptografski algoritam baziran na pseudoslučajnom generatoru RC4. Ovaj kriptografski algoritam je masovno primenjivan u telekomunikacionim standardima i protokolima u vremenu do 2015. godine. Svoju popularnost duguje izuzetno elegantnoj ideji promenljivih permutacija, kompaktnosti implementacije i efikasnosti u pogledu izvršavanja. Masovna popularnost je indukovalo isto tako masovnu pažnju kriptografske zajednice što je rezultovalo otkrivanjem brojnih slabosti različitog stepena uticaja i ozbiljnosti. Zbog otkrivenih slabosti i praktičnih napada koji su kompromitovali sisteme u kojima je ovaj kriptografski algoritma primenjen upotreba ovog algoritma je obustavljena 2015. godine. U radu je dat opis pseudoslučajnog generatora RC4, njegova analiza sa različitih aspekata i prikaz jednog dela rezultata koji su doveli do njegovog povlačenja. Primenom ideje promenljivih permutacija je realizovano još nekoliko kriptografskih algoritama ali su u svima pronađene bezbednosne slabosti koje ih diskvalifikuju za kriptografske primene.

Sa druge strane jednostavnost i elegancija ideje promenljivih permutacija ukazuje na mogućnosti njene primene. Stanovište sa kojim je započeto ovo istraživanje je bilo da problemi sa rešenjima koja su zasnovana na promenljivim permutacijama ne leži u njima kao takvima već u načinu na koji su promenljive permutacije upotrebljene. Sprovedeno istraživanje je potvrdilo zauzeto stanovište. Definisana je klasa slučajnih procesa koja odgovara promenljivim permutacijama a na osnovu nje je definisan pseudoslučajni generator koji koristi promenljive permutacije. Analiza definisane klase pseudoslučajnih generatora je pokazala da klasa pod određenim uslovima, koji su u radu eksplicitno navedeni, ima dobra kriptografska svojstva u pogledu raspodele verovatnoća izlaznog niza, korelacionih svojstava i dužine perioda.

S obzirom da je definisana klasa parametrizovana to omogućava realizaciju različitih uzajamno nekorelisanih konkretnih pseudoslučajnih generatora sa dobrim kriptografskim svojstvima. Izbor efikasnih i kompaktnih parametrizujućih pseudoslučajnih generatora kao rezultat daju efikasan, kompaktan i kriptografski pouzdan pseudoslučajani generator.

Potvrda polaznog stanovišta ovog istraživanja i dobijeni rezultat u formi parametrizovane klase pseudoslučajnih generatora koja ima dobra kriptografska svojstva ukazuju na mogućnost standardizacije ovog modela i na taj način postizanja uniformnosti i kompatibilnosti zaštitnih mehanizama u sajber prostoru.

## 5.2 Doprinosi rada

Kao što je ilustrovano rezultatima NESSIE i eSTREAM konkursa, nije lako dizajnirati kriptografski upotrebljiv sekvencijalni pseudoslučajni generator. Zahtevi koje nameće okruženje, kao što je implementacija na uređaje sa ograničenim resursima, mogu situaciju dodatno usložiti.

Istraživanje koje je rezultiralo ovim radom bavilo se problemom sinteze aditivnog sekvencijalnog kriptografskog algoritma baziranog na promenljivim permutacijama. Kako je po svojoj strukturi aditivni sekvencijalni kriptografski algoritam u suštini pseudoslučajni generator ovo istraživanje se fokusiralo na sintezu kriptografski pouzdanih pseudoslučajnih generatora.

Rezultati ovog istraživanja prikazani u ovom radu se mogu sublimirati kao sledeći doprinosi:

1. Definisana je klasa pseudoslučajnih generatora parametrizovana sa dva parametra. Ako se pseudoslučajni generator posmatra kao konačan automat sa izlazom parametri su funkcija promene stanja i funkcija izlaza. Kriptografske karakteristike definisane klase u pogledu raspodele verovatnoća izlaznog niza, korelacionih i algebarskih osobina te perioda izlaznog niza su dobre.

2. Kriptografske karakteristike definisane klase zavise samo od pripadnosti parametara skupu dobrih parametara a ne i od izbora konkretnih vrednosti parametara. Skup dobrih parametara okarakterisan je u Teoremi 25 u glavi 4. ovog rada. Brojnost skupa dobrih parametara ukazuje na mogućnost dobijanja praktično beskonačnog broja dobrih uzajamno nekorelisanih pseudoslučajnih generatora.

3. Mehanizam promenljivih permutacija omogućava sintezu vrlo efikasnih i kompaktnih pseudoslučajnih generatora primenljivih i u uređajima sa vrlo ograničenim resursima.

4. Na izvestan način definisana klasa pseudoslučajnih generatora predstavlja uopštenje generatora RC4 i po prikazanim rezultatima predstavlja rehabilitaciju ove ideje u kriptografskom miljeu.

Definisanje jedne ovakve klase kriptografskih pseudoslučajnih generatora u značajnoj meri unapređuje mogućnosti realizacije različitih, pa i vrlo visokih, nivoa bezbednosti podataka čak i na uređajima sa vrlo ograničenim resursima. Naravno i pored teorijski dokazivih dobrih kriptografskih karakteristika definisane klase pseudoslučajnih generatora u svakom konkretnom slučaju je neophodno sprovesti analizu uticaja i kompatibilnosti sa okruženjem u kojem se primenjuje.

Konačno ovaj rad se, za današnjicu, bavi vrlo aktuelnom i gorućom temom mehanizmima bezbednosti u sajber prostoru i IoT. Uspešan ishod ovog istraživanja nudi rešenje sa dobrim kriptografskim karakteristikama primenljivo u uređajima sa vrlo različitim dijapazonom računarskih resursa što potencijalno može imati posledice na standardizaciju i uniformnost primenjenih efikasnih kriptografskih pseudoslučajnih generatora

## 5.3 Otvorena pitanja

I pored postignutih rezultata u ovom istraživanju postoji nekoliko otvorenih pitanja čijim bi se rešavanjem unapredio postignuti rezultat:

1. Određivanje brzine konvergencije graničnog procesa u Teoremi 25 u terminima vrednosti parametara slučajnog procesa. Ovim bi se dobila univerzalna vrednost posle koje se raspodela izlaznog niza beznačajno razlikuje od uniformne raspodele, što je za primene značajna informacija.

2. Određivanje relacija između entropije primenjenog ključa i entropije izlaznog niza. Ova relacija, u slučaju pseudoslučajnog generatora, pokazuje koju količinu informacije o upotrebljenom ključu nose elementi izlaznog niza i omogućava određivanje tačke jedinstvenosti za dati pseudoslučajni generator.

3. Uspešan odgovor na prethodno pitanje omogućava definisanje nivoa bezbednosti klase pseudoslučajnih generatora u informaciono-teoretskom modelu.

Nabrojana pitanja i njihov značaj u ovom problemu opravdavaju dalji rad na istraživanju osobina definisane klase pseudoslučajnih generatora.

# Literatura


[1] R.A. Rehman, B. Khan, *IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors* **2018**, *18*, 2796.

[2] K. Salah, *The Era of Internet of Things, 2nd ed.*, Springer: Cham, Switzerland, 2019.

[3] A. Rayes, S. Samer, *Internet of Things from Hype to Reality, 2nd ed.*, Springer: Cham, Switzerland, 2019.

[4] H.F. Atlam, R.J. Walters, G.B. Wills, *Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues.* IJICR 2018, 9, 928–938.

[5] Costa, D.G. Figuerdo, S. G. Oliveira *Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions.* Cryptography 2017, 1, 4.

[6] Kambourakis, G. Marmol, F.G. Wang, *Security and Privacy in Wireless and Mobile Networks,* Future Internet 2018, 10, 18, doi:10.3390/fi10020018.

[7] S. Ziegler, *Internet of Things Security and Data Protection, 2nd ed.*, Springer: Cham, Switzerland, 2019.

[8] S. Cheruvu, A. Kumar, N. Smith, D.M. Wheeler, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment,* Apress: Berkeley, CA, USA, 2020.

[9] Z. Mahmood (Ed.), *Security, Privacy and Trust in the IoT Environment,* Springer: Cham, Switzerland, 2019.

[10] M.T. Banday, *Cryptographic Security Solutions for the Internet of Things*, IGI Global: Hershey, PA, USA, 2019.

[11] E. Shannon, *A mathematical theory of communication*, in The Bell System Technical Journal, vol. 27, no. 3, pp. 379-423, July 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[12] J. Katz, Y. Lindell, *Introduction to Modern Cryptography 3rd ed.*, CRC Press, 2020.

[13] G. J. Simmons et al., *Contemporary Cryptography: The Science of Information Integrity* IEEE Press, New York, USA ISBN 0-87942-277-7.

[14] A. Klein, *Stream Ciphers*, Springer London, 2013, ISBN 9781447150794.

[15] A. J. Menezes, S. A Vanstone, P. C. Van Oorschot, *Handbook of applied cryptography 5th. ed.*, CRC Press, Boca Raton 2001,isbn=9780849385230,0849385237.

[16] J. von zur Gathen, *CryptoSchool*, Springer-Verlag Berlin Heidelberg, 2015, isbn 978-3-662-48423-4.

[17] R. Rivest, *The RC4 encryption algorithm,* Rsa Data Secur Inc Doc No, 1992, 20: 86–96

[18] D. P. Anderson, R. G. Herrtwig, *Internet communication with end-to-end performance guarantees,* In: Telekommunikation und multimediale Anwendungen der Informatik. Berlin: Springer, 1991

[19] ETSI/SAGE. *Specification of the 3GPP confidentiality and integrity algorithms* UEA2&UIA2. Document 2: SNOW, 3G Specification, Version 1.1, 2006. http://www.gsmworld.com/using/algorithms/docs/etsi sage 06 09 06.pdf

[20] X. T. Feng *ZUC algorithm: 3GPP LTE international encryption standard,* China Inform Secur, 2011, 19: 45–46

[21] Bluetooth, *Specification of the Bluetooth system*, 2005. https://www.bluetooth.com/specifications/adoptedspecifications

[22] NESSIE, http://www.cryptonessie.org

[23] P. Ekdahl, T. Johansson, *A new version of the stream cipher SNOW*, In: Proceedings of International Workshop on Selected Areas in Cryptography, 2002. 47–61.

[24] P. Ekdahl, T. Johansson, *SNOW-a new stream cipher.* 2007. https://pdfs.semanticscholar.org/900e/081fa7ba0d0b45e36185e327e1081bf55d28.pdf

[25] European Commission, *First open NESSIE workshop,* 2000. https://www.cosic.esat.kuleuven.be/nessie/workshop/

[26] P. Hawkes , G. G. Rose, *Guess-and-determine attacks on SNOW,* In: Proceedings of International Workshop on Selected Areas in Cryptography, 2002. 37–46

[27] O. S. Markku-Juhani, *A time-memory tradeoff attack against LILI-128,* In: Proceedings of International Workshop on Fast Software Encryption, 2002.

[28] Y. Tsunoo, T. Saito, M Shigeri et al., *Shorter bit sequence is enough to break stream cipher LILI-128,* IEEE Trans Inform Theory, 2005, 51: 4312–4319.

[29] CRYPTREC Home Page (In English), http://www.cryptrec.go.jp/english/index.html

[30] National Information Security Center of Japan, *Guidelinesfor formulation and implementation of standards for information security measures for the central government computer systems* 2005. http://www.nisc.go.jp/eng/index.html

[31] H. Imai, *The future direction of the next round CRYPTREC,* WISA 2009 invited talk, Aug 2009 http://www.wisa.or.kr/

[32] *The eSTREAM Project.* http://www.ecrypt.eu.org/stream/.

[33] *Call for stream cipher primitives,* 2004. http://www.ecrypt.eu. org/stream/call/.

[34] M. Robshaw, O. Billet, (eds) *New stream cipher designs,* Lecture notes in computer science 4986. Springer, Berlin 2008

[35] H. M. Johansson, T. W. Meier, *Grain: a stream cipher for constrained environments,* Int J Wirel Mobile Comput, 2007, 2: 86–93

[36] C. D. Canniere, B. Preneel, *TRIVIUM specifications*, eSTREAM, ECRYPT Stream Cipher Project, 2006. http://www.ecrypt.eu.org/stream/

[37] S. Babbage, M. Dodd, *The stream cipher MICKEY 2.0,* eSTREAM, ECRYPT Stream Cipher Project, 2006. http://www.ecrypt.eu.org/stream/

[38] C. Berbain, O. Billet, A. Canteaut et al. *SOSEMANUK, a fast software-oriented stream cipher* In: New Stream CipherDesigns. Berlin: Springer, 2008. 98–118

[39] Boesgaard M., Vesterager M., Pedersen T. et al. *Rabbit: a new high-performance stream cipher*, In: Proceedings of International Workshop on Fast Software Encryption, 2003. 307–329

[40] Wu H. J., *The stream cipher HC-128,* In: New Stream Cipher Designs. Berlin: Springer, 2008. 39-47

[41] Carlet C., *Boolean Functions for Cryptography and Coding Theory,* Cambridge: Cambridge University Press, 2021. doi:10.1017/9781108606806

[42] Cusick T., Stanica P., *Cryptographic Boolean Functions and Applications, 2nd Edition*, Academic Press, 2017. ISBN: 9780128111291

[43] Wu C-K., Feng D., *Boolean Functions and Their Applications in Cryptography*, Springer-Verlag Berlin Heidelberg, 2016. ISBN: 978-3-662-48863-8

[44] Логачев, О.А., Сальников, А.А., Ященко В.В., *Булевы функции в теории кодирования и криптологии,* Серия: Новые математические дисциплины, М.: МЦНМО 2004 г. ISBN: 5-94057-117-4;

[45] Niederreiter H., Lidl R., *Introduction to finite fields and their applications,* Cambridge University Press, rev. ed., 2002. isbn 0521460948, 9780521460941

[46] Golomb S. W., *Shift register sequences, revised edition*, Aegean Park Press, Laguna Hills, 1982.

[47] Jansen C. J. A., *Investigations on nonlinear stream cipher systems: construction and evaluation methods,* PhD. thesis, Technical University of Delfth 1989

[48] Bernstein D. J., *The Salsa20 family of stream ciphers,* In New stream cipher. Springer, Berlin, Heidelberg, pp. 84-97, 2008.

[49] Bernstein D. J., *Chacha, a variant of Salsa20,* 2009. http://cr.yp.to/chacha/chacha-20080120.pdf

[50] Joux A., *Algorithmic Cryptanalysis,* Chapman & Hall/CRC, 2009. isbn:1420070029

[51] Stamp M., Low R. M., *Applied Cryptanalysis: Breaking Ciphers in the Real World,* Wiley-Interscience, 2007. isbn: 047011486X

[52] Siegenthaler T., *Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications,* IEEE Transactions on Information Theory. 30 (5): 776–780, 1984. doi:10.1109/TIT.1984.1056949.

[53] Golić J., *On the security of Shift register based keystream generators,* R. Anderson, editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 90–100, SpringerVerlag, 1994.

[54] Günther C.G, *Alternating step generators controlled by de Bruijn sequences,* Advances in Cryptology–EUROCRYPT '87 (LNCS 304), 5–14, 1988

[55] Coppersmith D., Krawczyk H., Mansour Y., *The Shrinking generator*, Advances in Cryptology–CRYPTO '93 (LNCS773), 22–39, 1994

[56] Kerckhoffs A., *La cryptographie militaire* Journal des Sciences Militaires, IX:5{38, January 1883. http://www.petitcolas.net/fabien/kerckhoffs.

[57] Kerckhoffs A., *La cryptographie militaire*, Journal des Sciences Militaires, IX:161{191, February 1883. http://www.petitcolas.net/fabien/kerckhoffs.

[58] NIST, *Federal Information Processing Standards Publication 197.* United States National Institute of Standards and Technology (NIST). November 26, 2001.

[59] Feller W., *An Introduction to Probability Theory and Its Applications. Vol. 1, 2.*, Wiley, 1968.

[60] Vernam G. S., *Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications,* Transactions of the American Institute of Electrical Engineers, 55: 109–115, 1926. doi:10.1109/T-AIEE.1926.5061224, S2CID 51639806

[61] Talbot J., Welsh D., *Complexity and Cryptography: An Introduction*, Cambridge University Press, USA 2006.

[62] Daemen J., Rijmen V., *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition,* Information Security and Cryptography, Springer 2020, ISBN 978-3-662-60768-8

[63] Knudsen L, *Contemporary Block Cipher*, in Lectures on Data Security, LNCS ed., I Damgard, Ed.: Springer Verlag, 1999, vol. 1561, pp. 105-126.

[64] Knudsen L. R., Robshaw M. J.B., *The Block Cipher Companion* Berlin Heidelberg: Springer Verlag, 2011.

[65] Aumasson J. P., *Analysis and Design of Symmetric Cryptographic Algorithms,* J. Lausanne: Ecole Polytecnique Federale de Lausanne, 2009.

[66] Bogdanov A., *Analysis and Design of Block Cipher Constructions,* Bochum: Universitat Bochum, 2009.

[67] Rueppel R. A., *Analysis and Design of Stream Ciphers*, Berlin: Springer Verlag, 1986.

[68] Rueppel R. A., *Security Models and Notions for Stream Ciphers*, in Proceedings of 2nd iMA Conference on Cryptography and Coding, Cirencester, England, 1989

[69] Д. И. Голенко, *Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах,* Москва: „Наука", Главная редакция физико-математической литературы, 1965

[70] Иванов М. А., Чугунков, И. В., *Теория, применение и оценка качества генераторов псевдослучайных последовательностей,* Москов: КУДИЦ-ОБРАЗ, 2003

[71] Biham E., Seberry J., *Py (Roo) : A Fast and Secure Stream Cipher Using Rolling Arrays*, eSTREAM: The ECRYPT Stream Cipher Project, Report 2005/023, Available at http://www.ecrypt.eu.org/stream/papers.html

[72] Keller N., Miller S., Mironov I., Venkatesan R., *MV3: A New Word Based Stream Cipher Using Rapid Mixing and Revolving Bufiers*, CT-RSA 2007, LNCS 4377, pp. 1-19, Springer-Verlag 2007.

[73] Wu H. *A New Stream Cipher HC-256*, In: Roy B., Meier W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017. Springer, Berlin, Heidelberg 2004. https://doi.org/10.1007/978-3-540-25937-4_15

[74] Wu H., Preneel B., *Key recovery attack on Py and Pypy with chosen IVs,* eSTREAM, http://www.ecrypt.eu.org/stream/papersdir/2006/052.pdf.

[75] Orumiehchi M.A., Mohebbipoor S.F., Ghodosi H., *Cryptanalysis of MV3 Stream Cipher,* In: Franklin M.K., Hui L.C.K., Wong D.S. (eds) Cryptology and Network Security. CANS 2008. Lecture Notes in Computer Science, vol 5339. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-89641-8_17

[76] Sekar G., Preneel B. *Improved Distinguishing Attacks on HC-256,* In: Takagi T., Mambo M. (eds) Advances in Information and Computer Security. IWSEC 2009. Lecture Notes in Computer Science, vol 5824. Springer, Berlin, Heidelberg 2009. https://doi.org/10.1007/978-3-642-04846-3_4

[77] Vizandan A., Sheikhzadegan J., Mirghadri A. *Cryptanalysis of the stream cipher HC-256 based on distinguishing attack*, Signal and Data Processing, -(2 (serial 14)), 13-22, 2010. https://www.sid.ir/en/journal/viewpaper.aspx?id=291159

[78] MacLaren M. D., Marsaglia G . *Uniform random number generation* J.ACM, vol. 15, pp. 83{89, 1965.

[79] Rrivest R., *6.857 Computer and Network Security Lectures and Handouts,* MIT: Cambridge, MA, USA,2008.

[80] Rivest R., Schuldt J. *Spritz—A Spongy RC4-Like Stream Cipher and Hash Function*, Available online: https://en.wikipedia.org/wiki/RC4\#cite_note-Rivest2014-14 (accessed on October 2019)

[81] Grosul A., Wallach D. S., *A Related-Key Cryptanalysis of RC4,* TR00-358, 2000. Dostupno na https://hdl.handle.net/1911/96275 april 2021.

[82] Matsuim., *Key collisions of the RC4 stream cipher,* In Orr Dunkelman, editor, FSE, volume 5665 of Lecture Notes in Computer Science, pages 38–50. Springer, 2009.

[83] Biham U., Dunkelman O., *Differential cryptanalysis in stream ciphers,* IACR Cryptology ePrint Archive, 2007:218, 2007

[84] Goutam P., Subhamoy M., *Permutation after RC4 key scheduling reveals the secret key*, In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, Selected Areas in Cryptography, volume 4876 of Lecture Notes in Computer Science, pages 360– 377. Springer, 2007

[85] Roos A., *A Class of Weak Keys in the RC4 Stream Cipher,* 1995. Two posts in sci.crypt, message-id 43u1eh$1j3@hermes.is.co.za

[86] Biham E., Carmeli Y. *Efficient reconstruction of RC4 keys from internal states,* In Kaisa Nyberg, editor, FSE, volume 5086 of Lecture Notes in Computer Science, pages 270–288. Springer, 2008.

[87] Akgün M., Kavak P., Demirci H., *New results on the key scheduling algorithm of RC4*, In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, INDOCRYPT, volume 5365 of Lecture Notes in Computer Science, pages 40–52. Springer, 2008.

[88] Khazaei S., Meier W., *On reconstruction of RC4 keys from internal states,* In Jacques Calmet, Willi Geiselmann, and Jörn Müller-Quade, editors, MMICS, volume 5393 of Lecture Notes in Computer Science, pages 179–189.Springer, 2008.

[89] Fluhrer S. R., Mantin I., Shamir A., *Weaknesses in the key scheduling algorithm of RC4,* In Serge Vaudenay and Amr M. Youssef, editors, Selected Areas in Cryptography, volume 2259 of Lecture Notes in Computer Science, pages 1–24. Springer, 2001.

[90] Korek, Need security pointers. Published online at http://www.netstumbler.org/showthread.php?postid=8903 6#pos%t89036, 2004.

[91] Korek, Next generation of WEP attacks? Published online at http://www.netstumbler.org/showpost.php?p=93942&post count=%35, 2004.

[92] Mantin I., *A practical attack on the fixed RC4 in the WEP mode,* In Bimal K. Roy, editor, ASIACRYPT, volume 3788 of Lecture Notes in Computer Science, pages 395–411. Springer, 2005.

[93] Klein A., *Attacks on the RC4 stream cipher,* Des. Codes Cryptography, 48(3):269–286, 2008. Published online in 2006, and accepted in WCC 2007

[94] Tews E., Weinmann R.-P., Pyshkin A., *Breaking 104 bit WEP in less than 60 seconds,* In Sehun Kim, Moti Yung, and Hyung- Woo Lee, editors, WISA, volume 4867 of Lecture Notes in Computer Science, pages 188–202. Springer, 2007.

[95] Vaudenay S., Vuagnoux M., P*assive-only key recovery attacks on RC4,* In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, Selected Areas in Cryptography, volume 4876 of Lecture Notes in Computer Science, pages 344– 359. Springer, 2007.

[96] Tews E., Beck M., *Practical attacks against WEP and WPA,* In David A.Basin, Srdjan Capkun, and Wenke Lee, editors, WISEC, pages 79–86. ACM, 2009.

[97] Sepehrdad P., Vaudenay S., Vuagnoux M., *Discovery and exploitation of new biases in RC4,* In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, pages 74–91. Springer, 2010.

[98] Sepehrdad P., Vaudenay S., Vuagnoux M., *Statistical attack on RC4 - distinguishing WPA*, In Kenneth G. Paterson, editor, EUROCRYPT, volume 6632 of Lecture Notes in Computer Science, pages 343–363. Springer, 2011

[99] Sepehrdad P., *Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-Lightweight Symmetric Primitives,* PhD thesis No. 5415, École Polytechnique Fédérale de Lausanne (EPFL), 2012. Available online at http://lasecwww.epfl.ch/~sepehrdad/Pouyan_Sepehrdad_PhD_Thesis.pdf.

[100] Popov *A. RFC 7465 Prohibiting RC4 Cipher Suites*, IETF: Fremont, CA, USA, 2015.

[101] Goutam P., Siddheshwar R., Maitra S., *On non-negligible bias of the first output byte of RC4 towards the first three bytes of the secret key,*. Des. Codes Cryptography, 49(1-3):123–134, 2008. Initial version in proceedings of WCC 2007

[102] Goutam P., Maitra S., *RC4 and its variants,* CRC Press, 2012

[103] Knudsen L. R., Meier W., Preneel B. Rijmen, V., Verdoolaege S., *Analysis methods for (alleged) RC4,* In Kazuo Ohta and Dingyi Pei, editors, ASIACRYPT, volume 1514 of Lecture Notes in Computer Science, pages 327–341. Springer, 1998.Serge

[104] Mister S., Tavares S. E., *Cryptanalysis of RC4-like ciphers,* In Stafford E. Tavares and Henk Meijer, editors, Selected Areas in Cryptography, volume 1556 of Lecture Notes in Computer Science, pages 131–143. Springer, 1998.

[105] Golić J. Dj., Morgari G., *Iterative probabilistic reconstruction of RC4 internal states,* IACR Cryptology ePrint Archive, 2008:348, 2008

[106] Shiraishi S., Ohigashi T., Morii M, *An improved internal-state reconstruction method of a stream cipher RC4*, In M.H. Hamza, editor, Communication, Network, and Information Security, Track 440–088, New York, USA, December 2003.

[107] Tomasević V., Bojanić S., Taladriz O. N. *Finding an internal state of RC4 stream cipher,* Inf. Sci., 177(7):1715–1727, 2007.

[108] Maximov A., Khovratovich D., *New state recovery attack on RC4*, In DavidWagner, editor, CRYPTO, volume 5157 of Lecture Notes in Computer Science, pages 297–316. Springer, 2008.

[109] Finney H., *An RC4 cycle that can't happen,* Post in sci.crypt, September 1994.

[110] Mantin I., A*nalysis of the stream cipher RC4,* Master's thesis, Weizmann Institute of Science, Rehovot, Israel, November 2001.

[111] Sen Gupta S., Maitra S., Goutam P., Sarkar S., *(Non-) Random Sequences from (Non-) Random Permutations—Analysis of RC4 Stream Cipher*, Journal of Cryptology 27, no. 1 (2014): 67-108

[112] Basu R., Ganguly S., Maitra S., Goutam P., *A complete characterization of the evolution of RC4 pseudo random generation algorithm,* J. Mathematical Cryptology, 2(3):257–289, 2008

[113] Mantin I., *Predicting and distinguishing attacks on RC4 keystream generator,*In Ronald Cramer, editor, EUROCRYPT, volume 3494 of Lecture Notes inComputer Science, pages 491–506. Springer, 2005.

[114] Jenkins R. J., *ISAAC and RC4,*. 1996. Available at http:// burtleburtle.net/bob/rand/isaac.html [last accessed on April 30, 2011

[115] Unkašević T., Banjac Z., Milosavljević M., *A Generic Model of the Pseudo-Random Generator Based on Permutations Suitable for Security Solutions in Computationally-Constrained Environments,*. Sensors. 2019; 19(23):5322. https://doi.org/10.3390/s19235322

[116] Stamp M., Low R., *Applied cryptanalysis : breaking ciphers in the real world.* Wiley: USA,2007.

[117] Privoult N., *Understanding Markov chains,* Springer Singapore: Singapore,2018.

[118] Sericola B., *Markov Chains- Theory, Algorithms and Applications,* Wiley: USA,2013.

[119] Wong Kk. K-H., Carter G., Dawson E. *An analysis of the RC4 family of stream ciphers against algebraic attacks,* In Boyd, C & Susilo, W (Eds.) Information Security 2010. Australian Computer Society, Australia, pp. 73-80. 2010.

[120] Unkašević T. *O jednoj slabosti RSA algoritma i mogućnostima za njenu zloupotrebu*, SYM-OP-IS '97,Bečići 1997.T

[121] Unkašević T, Perić M., Banjac Z., *O osetljivosti kriptografskih sistema,* Zbornik radova 23. telekomunikacioni forum TELFOR 2015, DRUŠTVO ZA TELEKOMUNIKACIJE – DT, BEOGRAD, ETF - Elektrotehnički fakultet

Univerziteta u Beogradu, IEEE Serbia & Montenegro COM CHAPTER, -1, vol. 23, no. 1, pp. 2.15 - 2.15, issn: 978-1-5090-054-8, udc: 519.2, Srbija, 24. - 25. Nov, 201

[122] Sakiyama K., Sasaki Y., Li Y., *Security of Block Ciphers: From Algorithm Design to Hardware Implementation (1st. ed.)*. Wiley Publishing.2015